Woodhouse Community Primary School Online Safety Policy

Reviewed: April 2023
To be ratified at the Curriculum & Standards Committee held on Summer 2023
Next review: April 2024

Designated Safeguarding Lead (s): (Rachael Smith Headteacher, Kirsty Ovington PSA, Vicky Curry Deputy Headteacher)

Named Governor with lead responsibility: Nigel Connah/ Suzanne Binks

Date written: (Autumn 2022)

Date agreed and ratified by Governing Body: September 2022

Date of next review: September 2023

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure.

Woodhouse Community Primary School

Online Safety Policy

1. Rationale

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

Students with internet access are more confident and have been shown to produce better-researched, more effective and well presented projects. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Some of the issues and risks are summarised below.

While many of the issues outlined in this section relate, primarily, to ICT use outside school, it is inevitable that some of the issues, when initiated outside school, will be bought back in and need to be dealt with accordingly by the school. For example, bullying via chat or text messages will impact upon relationships within school; obsessive use of the internet may impact upon the quality of schoolwork; and changes in the personality and general wellbeing of a pupil may indicate that they are involved in inappropriate or illegal behaviours online.

Schools therefore have a major responsibility to educate their pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

2. Aims

Our Online Safety Policy contains an Acceptable Use Policy which is written to give clear, concise guidelines to both pupils and staff that they can use to help them use the Internet safely and effectively to enhance teaching and learning.

The aims of this Online Safety policy are:

1. To allow all users to access and use the Internet for educational purposes. This can include E-Mail and World Wide Web facilities. The school activities can cover: Individual research /preparation of lessons/project work/homework assignments /communicating with other teachers and students.

2. To provide a mechanism by which staff and students are protected from sites, information, and individuals which would undermine the principles and aims of the school.

3. Provide rules which are consistent, and in agreement with the Data Protection Act.

4. Provide rules which are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.

3. Writing and reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for ICT, bullying and for child protection. It should be read in conjunction with these documents.

- The school Online Safety Coordinator is Senior Leader with responsibility for Online Safety (Rachael Smith/Victoria Curry), supported by the Online Safety Teacher (Zara Connor).
- Our Online Safety Policy has been written by Woodhouse Community Primary School involving staff, learners and parents/carers, building on the Kent County Council/The Education People/Durham County Council online safety policy template, with specialist advice and input as required.
- The Online Safety Policy and its implementation will be reviewed annually. Details of the Policy's approval and review are recorded in the Governing Body minutes.
- The Online Safety governor is Nigel Connah.
- It takes into account the DfE statutory guidance Keeping Children Safe in Education 2022, Early Years Foundation Stage framework 2022, Working Together to Safeguard Children and the Durham Safeguarding Children's Partnership procedures.
- The purpose of our online safety policy is to:
    - Safeguard and protect all members of Woodhouse Community Primary school's community online

- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

- Woodhouse Community Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

4. Teaching and learning

4.0 Classroom Use

- Woodhouse Community Primary School uses a wide range of technology. This includes access to:

o Computers, laptops, Ipads and other digital devices
o Internet which may include search engines and educational websites o Learning platform/intranet
o Email
o Games consoles and other games-based technologies, Digital cameras, web cams and video cameras.

- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

o The Smoothwall filtering system used in school ensures that when using Google it is automatically set to safe search. This reduces but does not eliminate the risk of links to inappropriate content.

- We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information.

- Supervision of learners will be appropriate to their age and ability.

- **Early Years Foundation Stage and Key Stage 1**

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the

learning outcomes planned for the learners' age and ability.

- **Key Stage 2**
  - Learners will use age-appropriate search engines and online tools.
  - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners' age and ability.

4.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

4.2 Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

4.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5. Managing Internet Access

5.1 Information system security

School ICT systems capacity and security will be reviewed regularly.

- Security strategies are in line with national guidance.
- Virus protection is updated regularly

5.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 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.

5.3 Published content and the school web site

- Our website includes the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Senior Leaders responsible with responsibility for published content and the school website (Rachael Smith and Victoria Curry), who will take overall editorial responsibility and ensure that content is accurate and appropriate.

5.4 Publishing pupil's images and work

- Photographs showing pupils will only be included when the pupils cannot be identified by name. Pupils' full names will be used on the website but not alongside a photograph. Photographs can only be published with the permission of parents. This permission will be included as part of the pupil registration information when a child joins our school.
- Pupil's work can only be published with the permission of the pupil and parents. This permission will be included as part of the pupil registration information when a child joins our school.

5.5 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Parental permission for this use of the internet will be sought as part of the pupil registration information when a child joins our school.

5.6 Managing filtering

- IT Systems (school system manager) have a comprehensive filter and monitoring system in palace to protect pupils for harmful online materials (Smoothwall).
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- Regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. This is through the technical support Service Level Agreement (ITSS).

5.7 Managing emerging technologies

- Adults working in school are not allowed to use mobile phones while working with children. They will be kept out of sight.
- Children are not permitted to bring mobile phones in to school without specific written permission from the school and parents.
- The sending of abusive or inappropriate text messages is forbidden (see anti-bullying policy)

5.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act.

6. Policy Decisions

6.1 Authorising Internet access

- The school has the right to withdraw access to the internet if deliberate inappropriate use is found.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form on entry to school.

6.2 Assessing risks

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. Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices. All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

- The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.
- The school will monitor which sites are being accessed through the implementation of 'Smoothwall', provided through our IT provider 'ITSS. ' Deliberate and/or repeated attempts to access inappropriate sites are monitored by IT Systems and Support, who reports to the HS.

6.3 Handling Online Safety complaints

- Complaints of internet misuse will be dealt with in line with the school's Complaints Policy.
- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school Child Protection Policy, through the Head of School as designated Child Protection Officer.
- Pupils and parents will be informed of the complaints procedure.

6.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to Online Safety, for example liaison with Family Learning before using school facilities.

7. Communications Policy

7.1 Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in classrooms and discussed with pupils at the start of each year and regularly reviewed
- Pupils will be informed that network and internet use will be monitored.

7.2 Staff and the Online Safety policy

- All staff will be provided with access to our Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff must not use the school's internet facilities for personal use.

7.3 Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, Class Dojo and on our website, as well as when registering pupils who join the school.
- Parental guidance leaflets will be sent to parents when necessary.

Communication with children (including the use of technology)

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.)
This means adults should:

- not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work

- not give out their personal details
- use only equipment and Internet services provided by the school or setting
- follow their school / setting's Acceptable Use policy
- ensure that their use of technologies could not bring their employer into disrepute

Youth Produced Sexual Imagery (Sexting).

The UK Council for Child Internet Safety (UKCCIS) Education Group has recently published sexting advice for schools and colleges. The department provides searching screening and confiscation advice for schools. Guidance produced by UKCCIS 'Sexting in Schools and Colleges'

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

This is fully implemented within the Woodhouse Community Primary School Safeguarding Policy.

Online abuse

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- bullying/cyberbullying

- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

Extract from Durham County Council Online Safety Policy template

Social Media

a. Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Woodhouse Community Primary School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Woodhouse Community Primary School community are expected to engage in social media in a positive, safe and responsible manner.
  - o All members of Woodhouse Community Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control staff access to social media whilst using setting provided devices and systems on site.
  - o The use of social media during setting hours for personal use *is* permitted during staff break/lunchtimes away from the classroom setting and away from learners.

Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of Woodhouse Community Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

b. Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - o Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - o Setting the privacy levels of their personal sites. o Being aware of location sharing services.
  - o Opting out of public listings on social networking sites. o Logging out of accounts after use.
  - o Keeping passwords safe and confidential.
  - o Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Woodhouse Community Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers.

All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.

- o Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL and the headteacher.
- o If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.

- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

C. Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore, we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
  - o Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
  - o To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
  - o To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
  - o Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
  - o To use safe passwords.
  - o To use social media sites which are appropriate for their age and abilities. o How to block and report unwanted communications.
  - o How to report concerns both within the setting and externally.

d. Official Use of Social Media

- Woodhouse Community Primary School official social media channels are: Facebook page
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - o The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.
  - o Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure that they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
    - Inform their line manager, the DSL (or deputy) and/or Rachael Smith/Victoria Curry.

Staff ICT Acceptable Use Policy 2022

As a professional organisation with responsibility for children's safeguarding it is importa that all staff take all possible and necessary measures to protect data and informati systems from infection, unauthorised access, damage, loss, abuse and theft. All members staff have a responsibility to use the school's computer system in a professional, lawful, a ethical manner. To ensure that members of staff are fully aware of their professioi responsibilities when using Information Communication Technology and the school systen they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should consistent with the school ethos, other appropriate policies and the Law.

1) I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, digital cameras, email and social media sites.

2) School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to compute material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3)

   a) Staff mobile phones will never be used for any reason when children are present

   b) Mobile phones should only be used for communication when not working with children.

   c) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

   d) In the unlikely event of needing to contact a parent directly, a school mobile phone will be issued to the member of staff concerned.

4) I understand that any hardware and software provided by my school for staff use can only be used by members of staff

5) Personal use of school ICT systems and connectivity is only permitted with the consent of the headteacher,

6) To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

7) I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 10 or more characters, does not contain a dictionary word and is only used on one system).

8) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

9) Data Protection {*We have a separate Data Protection Policy – some of the key guidance should be contained within the Staff AUP*}

   a) I will ensure that any personal data is kept in accordance with the General Data Protection Regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any personal data on portable devices (USB, laptops, tablets etc) {Secure means of transporting data are encrypted laptop / encrypted USB memory / encrypted HDD / approved cloud based system }

   b) If I choose to use a portable device (Phone, Tablet etc...) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

   c) I will not transfer sensitive personal information from my school e-mail account (e.g. EHCP's, SEND reports, Safeguarding Reports, Medical Information) UNLESS the information is encrypted/ password protected.

   d) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones)

   e) Digital Images or videos of pupils will not be taken away from the school premises without express permission from DSL for a school based purpose

   f) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

11) I will respect copyright and intellectual property rights.

12) Social Media. .

   a) I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

   b) I will not communicate with pupils or ex-pupils using social media without the express permission of the Headteacher.

   c) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. *This would include any relatives of current pupils that are my "friends" on a social media site.*

d) My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

e) I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children's online safety to the Designated Safeguarding lead (DSL) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites the designated lead for filtering as soon as possible

14) I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (named contact) as soon as possible

15) I will promote Online Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

16) If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the DSL or their deputy.

17) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ..... Print Name: ..... Date: .....

Accepted by: ..... Print Name: .....

Online Safety Scheme of Work- Kapow						
Year Group	**Autumn 1**	**Autumn 2**	**Spring 1**	**Spring 2**	**Summer 1**	**Summer 2**
EYFS		Smartie the Penguin- Story A		Smartie the Penguin- Story B		Jessie and Friends- Watching Videos (Watch video at following link) https://www.thinkuknow.co.uk/parents/jessie-and-friends-videos/
Year 1	Smartie the Penguin- Story A (Year 1)	Smartie the Penguin- Story B (Year 1)	Using the Internet Safely	Online Emotions	Always be kind and considerate	Posting and sharing online
Year 2	Recap of Year 1 Online Safety- Assessment Knowledge Catcher.	What Happens When I Post Online?	How Do I Keep My Things Safe Online?	Who Should I Ask?	It's My Choice	Is It True?
Year 3	Recap of Year 2 Online Safety- Assessment Knowledge Catcher.	Beliefs, Opinions and Facts On the Internet.	When Being Online Makes Me Upset	Sharing of Information	Rules of Social Media Platforms	Assessment- Quiz
Year 4	Recap of Year 3 Online Safety- Assessment Knowledge Catcher. **What Happens When I search Online?**	How Do Companies Encourage Us to Buy Online?	Fact, Opinion Belief?	What is a Bot?	What is My Tech Timetable Like?	How Can I Be Safe and Respectful Online? Assessment- Quiz
Year 5	Recap of Year 4 Online Safety- Assessment Knowledge Catcher. **Online Protection**	Online Communication	Online Reputation	Online Bullying	Online Health	Assessment- Quiz
Year 6	Recap of Year 5 Online Safety- Assessment Knowledge Catcher. **Life Online**	Sharing Online	Creating a Positive Online Reputation	Capturing Evidence	Password Protection	Think Before You Click Assessment-Quiz

Taken from Kapow Computing that links to Educated for a Connected World 2020 Framework.