



Confident, Resilient, Ambitious, Brilliant

Suffield Park Infant and Nursery School

Online Safety Policy

Contents:

- Aims
- Legal Framework
- Roles and Responsibilities
- Maintenance of ICT Systems
- Educating Pupils about Online Safety
- Educating Parents/Carers about Online Safety
- Remote and Home Learning
- Cyberbullying
- Responding to Specific Online Safety Concerns
- Examining Electronic Devices
- Acceptable use of the Internet and devices in School and off the School Premises
- How the School will Respond to Issues of Misuse
- School Website
- Online Hoaxes and Harmful Online Challenges
- Social Networking/Social Media
- Training
- Links to other Policies
- Appendix 1 ICT Code of Conduct
- Appendix 2 Tapestry Use Policy and Risk Assessment
- Appendix 3 Letter to Parents/Carers
- Appendix 4 Online Safety Rules for Pupils

Aims:

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

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

Therefore Suffield Park Infant and Nursery School aims to:

- Have robust processes in place to ensure the online safety of Pupils, Staff, Volunteers, Governors and Visitors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legal Framework:

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2020'

- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- It also refers to the DfE's guidance on protecting children from radicalisation.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- The policy also takes into account the EYFS, and National Curriculum Computing and RSE programmes of study.

Roles and Responsibilities:

- The Governing Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.
- All Governors will:
- Take responsibility for the security of ICT systems and electronic data they use or have access to. Agree and adhere to the terms in the Suffield Park and Infant Schools 'ICT Code of Conduct' (see Appendix 1). Maintain a professional level of conduct in their personal use of technology, internet use and social media/social networking, inside and outside of school.
- Ensure that there are appropriate filtering and monitoring systems in place in School/Nursery.
- The Governor who oversees Computing/Online Safety is Viv Lennox.
- The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction, safeguarding training and continued professional development.
- Supporting staff to ensure that online safety is embedded throughout the curriculum and school/nursery so that all pupils can develop an appropriate understanding of online safety.

The Designated Safeguarding Lead:

- Working with the Headteacher, Computing/Online Safety Lead and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately.
- Updating and delivering staff training on online safety alongside Computing/Online Safety Lead.
- Liaising with other agencies and/or external services if necessary.
- Understanding the risks associated with online safety for adults and pupils, and can recognise additional risks that pupils who are vulnerable, SEND face online (along with SENDCO).

Computing/Online Safety Lead:

The Computing/Online Safety Lead is responsible for:

- See Designated Safeguarding Lead responsibilities as they will support alongside these.
- Writing Online Safety Policy, ICT Code of Conduct, Tapestry Use Policy and Risk Assessment, Writing Rules for Online Safety for Pupils – displayed around school and sent home for parents (signed slip returned).
- Leading online safety events e.g. Safer Internet Day.

- Supporting staff with teaching and learning in Online Safety e.g. 3iis, progression map, answering questions, monitoring, observations etc.
- Helping to tackle issues arising in school with a whole school based response e.g. a concern is flagged in Reception (children watching inappropriate content on YouTube at home – respond with whole school approach to address issue).
- Providing information for Parents/Carers on online safety e.g. Termly Online Safety Newsletter, Online Safety tab on school website, invited to take part in events like Safer Internet Day, posters relating to Online Safety displayed around school e.g. PEGI ratings. Information passed on when relevant e.g. on parental controls, information leaflets from companies, latest crazes e.g. Fortnite or internet based challenges etc.
- The Computing/Online Safety Lead is Michelle Mitchell.

All Staff, Volunteers and Visitors:

- Maintaining an understanding of this policy and implementing this policy consistently.
- Take responsibility for the security of ICT systems and electronic data they use or have access to. Agree and adhere to the terms in the Suffield Park and Infant Schools 'ICT Code of Conduct' (see Appendix 1) and Tapestry Use Policy and Risk Assessment (see Appendix 2). Maintain a professional level of conduct in their personal use of technology, internet use and social media/social networking, inside and outside of school.
- Working with the DSL and Computing/Online Safety Lead to ensure that any online safety incidents are logged and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are reported and dealt with appropriately.
- Understanding the risks associated with online safety adults and pupils, and can recognise additional risks that pupils who are vulnerable, SEND face online.
- Model good online behaviours and where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum and across the school.
- Staff to be mindful about the online resources that they use and show to pupils.
- Pupils are clearly told expectations when using electronic devices/are online e.g. where they can be used, where they cannot be taken, where they need storing after use, what they can go on etc.

Parents/Carers:

- When their child starts at Suffield Park Infants school they are given a letter (see Appendix 3) detailing our Online Safety rules for Pupils (see Appendix 4), which they are asked to discuss with their child. They are asked to sign and return a slip.

Pupils:

- See Appendix 4 for a copy of Online Safety Rules for Pupils – which are displayed around School and referred to during teaching etc.

Maintenance of ICT systems:

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).
- We have a contract with ICT solutions, through this we have access to their support team and we have a weekly visit to the school from a Technician who ensures that the school's ICT systems are secure, backed up and protected against viruses and malware, and that such safety mechanisms are updated regularly. They monitor the school's ICT systems. The Technician also provides technical support and advice.
- Through ICT Solutions we have in place appropriate internet filtering and antivirus software, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. This also includes blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Educating Pupils about Online Safety:

Pupils will be taught about online safety as part of the curriculum:

- Objectives are taken from the National Curriculum for Computing and RSE.
- Progression map created to inform staff planning and progression of skills and knowledge in Online Safety.
- Online safety is embedded throughout the curriculum and addressed whenever necessary.
- Pupils are reminded of Online Safety Rules, which are displayed in classrooms and used in IWBs/PowerPoints etc.
- Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.
- The underpinning knowledge and behaviours pupils learn through the curriculum include the following: How to evaluate what they see online, how to recognise techniques used for persuasion, acceptable and unacceptable online behaviour, how to identify online risks, how and when to seek support, how to identify when something is deliberately deceitful or harmful, how to recognise when something they are being asked to do puts them at risk or is age-inappropriate.
- Online safety teaching is always appropriate to pupils' ages and developmental stages.
- New online risks pupils may face are considered and addressed as is appropriate.

Educating Parents/Carers about Online Safety:

- See Appendix 3 for a copy of the letter parents/carers are given when their child starts Suffield Park Infant School.
- Providing information for Parents/Carers on online safety e.g. Termly Online Safety Newsletter, Online Safety tab on school website, invited to take part in events like Safer Internet Day, posters relating to Online Safety displayed around school e.g. PEGI ratings. Information passed on when relevant e.g. on parental controls, information leaflets from companies, latest crazes e.g. Fortnite or internet based challenges etc.
- Online Safety Policy available on website.
- Parents/Carers encouraged to discuss any concerns they have over their child's online behaviour at home/school with Staff. Staff will also discuss any concerns they have regarding a pupil's online behaviour at home/school with Parents/Carers.

Remote and Home Learning:

- Please see Remote and Home Learning Policy.
- Live Meets – Parents (see Appendix 5) and Staff (see Appendix 6) issued with guidance.
- Staff also to refer to their ICT Code of Conduct, Tapestry Use and Risk Assessment and Staff Code of Conduct.

Cyberbullying:

- **Bullying** is defined as the repetitive, intentional harming of one person or group by another person or group.
- Bullying is, therefore: Deliberately hurtful, repeated, often over a period of time, and difficult to defend against.
- Cyberbullying is bullying that takes place online, such as through social networking sites, social media, messaging apps or gaming sites.
- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. This will be at an age appropriate level for our pupils.
- The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Again, this will be at an age appropriate level for our pupils.
- When appropriate, the school will give information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyberbullying, the school will follow appropriate procedures. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

- The Headteacher and DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
- Cyberbullying against staff and pupils is not tolerated.

Responding to Specific Online Safety Concerns:

- The School recognises that there are many concerns including, but not restricted to:
- Cyberbullying. Online sexual violence and sexual harassment between children (peer-on-peer abuse). Upskirting. Sexting and the sharing of indecent imagery of pupils. Online abuse and exploitation. Online hate. Online radicalisation and extremism.
- The School will deal with these in line with the Safeguarding Policy.

Examining Electronic Devices:

- School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
- When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
 - Cause harm, and/or
 - Disrupt teaching, and/or
 - Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
 - Delete that material, or
 - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
 - Report it to the police
- Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the school's COVID-19 risk assessment.
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the Internet and devices in School and off the School Premises:

- Staff, Governors and Volunteers – signing the ICT Code of Conduct and Tapestry Use and Risk Assessment (if appropriate to their role).
- Visitors are expected to adhere to taking responsibility for the security of ICT systems and electronic data they use or have access to. Also to adhere to the schools 'ICT Code of Conduct' when they are on-site.
- Parents/carers are given a letter to read, discuss with their child and sign when their child starts Suffield Park Infant School.
- We will ensure that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

How the School will respond to issues of misuse:

- Where a pupil misuses the school's ICT systems, devices or internet, action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- Where a staff member misuses the school's ICT systems or the internet, or misuses a digital device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

School Website:

- The Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
- The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.
- Images and videos are only posted on the website if the provisions in the Photography Policy are met and consent is given.

Online Hoaxes and Harmful Online Challenges:

- For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.
- For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.
- Pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, this is at an age appropriate level for our pupils.
- Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the Headteacher/DSL immediately.
- The Headteacher/DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils.
- The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils’ exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

Social Networking/Social Media:

- Social Networking/Social Media activities are conducted online such as blogging, websites, Facebook, Twitter, YouTube, LinkedIn, Snap Chat, TikTok etc.
- Staff at Suffield Park Infants and Nursery School have a responsibility to ensure that they protect the reputation of the School, and to treat colleagues and members of the school community with professionalism and respect.
- See ICT Code of Conduct for further information on Social Networking/Social Media use.

Training:

- Staff will receive ICT Code of Conduct, Tapestry Use and Risk Assessment and Online Safety Policy at Induction. Plus they will receive updated copies if things change.
- Staff receive Safeguarding Training which includes Online Safety and updated information from Keeping Children Safe in Education related to this.
- Staff are updated on developments/requirements of the EYFS, Computing and RSE curriculum.
- Relevant information disseminated to Staff.
- Specific training needs addressed.

Links with other Policies:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures

- Data protection policy and privacy notices

Appendix 1 ICT Code of Conduct

Staff, Governor, Volunteer and Visitor 'ICT Code of Conduct' for *Suffield Park Infant and Nursery School*

This 'ICT Code of Conduct' has been created to ensure that Staff/Governors/Visitors understand their responsibilities and adhere to this policy when using school-owned digital devices and personal digital devices, whether on or off the school premises. Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined. Please ensure that you have read this in conjunction with the Online Safety Policy, the Tapestry Use Policy and Risk Assessment. Any concerns or clarification should be discussed with **Nichola Stewart or Michelle Mitchell**.

- **All Staff, Governors, Volunteers and Visitors:**
- Understand that ICT includes a wide range of systems, platforms, internet and digital devices e.g. computer, desktop, phone, laptop, tablet, chrome book, digital camera etc.
- Understand it is a **disciplinary offence** to use the School ICT system and equipment for any purpose not permitted by its owner.
- Will ensure that any data of the School, Nursery, Staff, Governors, Pupils, Families, Volunteers, Visitors, Members of the School Community etc is stored in line with the GDPR on and off the school premises. They will ensure any data stored on digital devices is encrypted/password protected.
- Will only use School/Nursery issued memory sticks if one is needed. These are to be returned to Lindsay Kerry. Memory sticks should also only be used for the transport of data to and from somewhere. The data on it should be deleted as soon as possible. The 'Shared Drive' and 't-drive' can be used for sharing information, documents etc.
- Will use school-owned devices, where possible, when completing School/Nursery based work. However, personal devices may be used if needed.
- Understand that school owned devices e.g. ipad, laptops etc, supplied by the school will only be used for their intended schoolwork use and in line with their role as an employee. The device is not be used for personal use or by anyone else.
- Understand that they are responsible for all activity carried out under their username, as everyone is provided with their own personal logins.
- Will not disclose any passwords provided to them by the School/Nursery or other related authorities.
- Will not disclose to anyone any passwords which they have to log on to websites, digital devices etc. Passwords should be strong and regularly updated.
- Are responsible for the digital devices they are working on, websites and software they are logged into etc. being locked or logged out of when they are not in use or are unattended etc.
- Are responsible for the safe storage of digital devices at School/Nursery and when taken off-site e.g. when at home laptop is stored out of sight in a cupboard for example.
- Immediately report any damage or loss of devices to Nichola Stewart or Michelle Mitchell.
- Will only use the approved email system(s) for any school business which have been provided. This will normally be the nsix email. All Staff, Governors and Visitors understand that all email accounts, usernames etc belong to the school. All Staff, Governors and Visitors will ensure that all their school generated electronic communications are appropriate and compatible with their role.
- Will delete any chain letters, spam and other emails from unknown sources without opening them.
- Will not install or alter any hardware or software on any school owned device without the permission of Nichola Stewart or Michelle Mitchell (*who will seek advice if necessary*). Staff will only use websites/apps that are GDPR-compliant and from reputable sources.
- Understand that their permitted use of the Internet, digital devices and other related technologies is monitored and logged and will be made available, on request, to their Line Manager or Headteacher in line with any disciplinary procedures. This relates to all school owned digital devices provided by the school.

- Will only use the school’s email / Internet / Intranet / Learning Platforms / Educational Websites / School work based Websites and any related technologies and devices for uses permitted by the Headteacher or Governing Body.
- Photographs/Videos of Pupils will only be taken, stored and used for purposes in line with school policy. These must be taken with a school-issued digital device. Photographs/Videos will not be downloaded to personal devices or distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Headteacher.
- Will comply with copyright and intellectual property rights.
- Will report any incidents of concern regarding staff use of technology, digital devices, online behaviour, social media/social networking and/or children’s safety to the Headteacher or DSL in line with the school’s Safeguarding Policy and procedures.
- Understands that if they are representing the school online, e.g. through blogging or on school social media account, school website, Tapestry etc, they will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- Ensure that any contact with parents/carers/pupils is done through authorised school contact channels.
- Understand that when a phone call is made to parents/carers it is done on a school phone. If this is not possible e.g. working remotely – then the number you are calling from must be withheld.
- Will not communicate with parents/carers about School related matters through personal social media/social networking accounts/sites or messenger services e.g. Facebook, Messenger, What’s App, Text etc.
- Understand that any digital devices must not be taken to the toilet/sink area or areas where people are changing.
- Will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make/receive calls and use the device in specific areas, at designated times, away from pupils.
- All Staff should not use any social media during their school working hours, this includes break time. During your designated lunchtime appropriate use is permitted of social media.
- Will not browse, download, upload or distribute any material that could be considered offensive, illegal, discriminatory, and confidential or that might bring the school into disrepute. This includes what you are posting, commenting on and liking on Facebook or other social media/social networking sites.
- Will ensure that the necessary privacy settings are applied to any social networking/social media sites.
- All personal devices **brought into school** must be password protected.

I certify that I have read and understood this agreement and ensure that I will abide by the terms outlined

Full Name:.....(printed)

Position in School:.....

Signature:.....

Date:.....

Appendix 2 Tapestry Use Policy and Risk Assessment

| This Policy and Risk Assessment is to outline expectations for all Staff when using Tapestry either in School or Off School Premises . This includes all Staff across our setting Admin, Head Teacher, SLT, EYFS (Nursery and Reception) and Key Stage One. | |
|---|---|
| Identifying the hazards - assessing the risk | Control measures – reducing the risk |
| Staff | <ul style="list-style-type: none"> • Safeguarding Training attended by all staff. • All staff fully DBS checked. • Tapestry Use Policy and Risk assessment shared with all staff and signed. • Staff have ICT Code of Conduct on induction. |

| | |
|---|---|
| <p>Tapestry website and Tapestry app accessed through ipads – This applies at School and Off School Premises.</p> | <ul style="list-style-type: none"> • Teachers and Teaching Assistants have access to Tapestry via the website and the app. • Teachers have manager permissions but Teaching Assistants do not. • All staff in Nursery access Tapestry via the website and the app. • In Nursery Room Leaders, Admin and Management have manager permissions. On occasion Nursery Manager (Hayley Powell) will elevate a Nursery Assistant’s access to management level for a specific task e.g. if staff are isolating but well enough to work (this is always time limited and for a specific task). • Tapestry website can only be accessed using individual staff nsix email and self-chosen ‘strong’ password using the secure Network when in School, but will be accessed through a personal internet connection when working off School Premises. • The app is accessed via a username and PIN (different for each member of staff) which is not saved to the device. • Staff can access Tapestry through school and personal devices but guidelines must always be adhered to. • School has designated PIN protected ipads for Staff use, which has the Tapestry app on – for use in school and these will sometimes be taken home for staff use of Tapestry. • Staff will log out of Tapestry website or app when they have finished what they are doing on Tapestry. • Staff will not disclose their Tapestry login details, password or PIN to anyone, not even another member of staff. |
| <p>Taking of and sharing of Photographs, Videos and sharing of any information – This applies at School and Off School Premises.</p> | <ul style="list-style-type: none"> • Staff to delete photographs and videos which are stored on devices as soon as they have been added to Tapestry and/or stored on the server. • Staff will not download any images or information to personal computers/tablets/mobile phones etc. • Staff will not share the information stored (including photographs, videos, observations, personal information, Tapestry assessment information etc) with anyone other than the relevant staff members who need to know it. |
| <p>Use of School devices e.g. ipads, laptops, any school owned device – This applies at School and Off School Premises.</p> | <ul style="list-style-type: none"> • Staff will use school-owned devices, where possible, when accessing Tapestry. However, personal devices may be used if needed. • School owned devices e.g. ipad, laptops etc, supplied by the school will only be used for their intended schoolwork use and in line with their role as an employee. The device is not be used for personal use or by anyone else. |

| | |
|--|---|
| | <ul style="list-style-type: none"> • In school, staff ipads to be kept out of reach/sight when they are not being used. Ipads in school to be stored overnight out of sight or in locked charging cabinet. • At home, staff ipads, laptops etc to be stored out of sight. • No devices to be taken into the toilet/sink area. • Staff to immediately report the loss or damage of any device. |
| <p>When filming yourself for Tapestry – This applies at School and Off School Premises.</p> | <ul style="list-style-type: none"> • Staff will use school-owned devices for filming, where possible but there may be times when they need to use a personal device to do this. • Staff will ensure they film themselves (this could be reading a story, sharing information, a pre-recorded lesson etc) in an appropriate location – either the classroom, or an appropriate location at home. Keeping in mind the background, clothing and that it is a quiet environment. • Staff to watch back filmed videos before they are uploaded to Tapestry. |
| <p>Using of Tapestry – This applies at School and Off School Premises.</p> | <ul style="list-style-type: none"> • Staff to add professional comments and text to Tapestry, taking care to check for spelling and grammar. • Teachers approve Teaching Assistant observations before they are published to Tapestry. • In Nursery, all staff with a key person responsibility (with addition of Hayley, Kathryn and Emmalene) can publish observations directly to the journal, they are not approved by another member of staff. This is due to the number of children in Nursery. • In Nursery students, bank staff, those without key children cannot publish to the journal. They can create observations but another member of staff has to approve and add to the journal. • Staff to report any safeguarding concerns about what they have seen uploaded to/commented on Tapestry from parents/carers/family/friends following school procedures of CPOMS. • Staff to know that they have a duty to report anything they see (e.g. on a devices, an observation or comment uploaded etc) from another member of Staff that raises a concern in line with the ‘Whistle Blowing’ policy. |
| <p>Parent/Carer</p> | <ul style="list-style-type: none"> • Full parental/carers permission gained and signed, for child to be on Tapestry. • Parents sign to say that they or any other named contact will not share photographs or videos via social media. |

Print Name

Signed

Date

Appendix 3 Letter to Parents/Carers
Dear Parent/Carer,

Technology and Computing includes the use of the internet, email, computers, ipads, tablets, digital cameras and other technologies. These have become an important part of learning in our school and of children's everyday lives.

Please would you read the attached 'Keeping Safe Online' rules and discuss these with your child.

On the 'Online Safety Reply slip' please read the parent/carer information. Then fill out your child's details and sign to say that you have read and discussed the 'Keeping Safe Online' rules with your child and that you have read the Parent/Carer information and that you agree to this. Please return slips to class teachers.

If you have any questions please speak to your child's class teacher or myself.

Thank you for your support.

Mrs Nichola Stewart
Head Teacher

Online Safety reply slip

I have discussed the 'Keeping Safe Online' rules and the safe use of digital technologies with my child. My child agrees to follow the 'Keeping Safe Online' rules and I (parent/carer) will support the safe use of the internet and digital technologies at Suffield Park Infant and Nursery School.

Parent/Carer information

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, employing appropriate teaching practice and teaching online safety skills to pupils. I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son's/daughter's online behaviour. I will support the school by promoting safe use of the Internet and digital technologies at home and will inform the school if I have any concerns over my child's online behaviour.

Child's name.....

Class.....

Parent Email Address.....

Parent/Carer Signature.....






Date.....

Appendix 4 Online Safety Rules for Pupils

Devices which I might go online with:



Keeping Safe Online

| | |
|---|--|
|  | I will look after the devices that I am using and will follow the rules for keeping safe. |
|  | I will talk to an adult if I see something that I do not like. I will tell an adult if something pops up when I am using a device. |
|  | I will ask an adult if I am allowed on a new website or online game. |
|  | I know that it is important to play games which are suitable for my age. |
|  | I will think about how much time I spend on the computer because I know that it is important to also stay active. |
|  | Just like in real life, I will be kind when I am online. |
|  | I will not play games online with people that I do not know and I will not send <u>them</u> messages because these people are strangers. |
|  | I will not share personal information with people (full name, date of birth, address, phone number, where I go to school). |
|  | I am learning about the safety tools to <u>block</u> , report or flag up. |