Moulton Primary School

Acceptable Use Policy

2023-2024

PERSON RESPONSIBLE FOR POLICY:	**MISS LAUREN JONES**
APPROVED:	**FULL GOVERNING BODY**
TO BE REVIEWED:	**JANUARY 2025** (or before if needed)

Section 1: What is an AUP (Acceptable Use Policy)?

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within a school or other educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within an area. At present the internet technologies used extensively by young people in both home and school environments include:

- Websites/blogs
- Social networking and chat rooms
- Gaming/forums on Xbox live etc.
- Music downloading
- Mobile phones with wireless connectivity
- Email and instant messaging
- Learning platforms
- Video broadcasting
- Apple/Windows apps

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. This policy should also provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It explains procedures for any unacceptable use of these technologies by adults, children or young people.

Why have an AUP?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Commercial issues with spam and other inappropriate e-mail
- Online grooming
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device
- Viruses
- Cyber-bullying
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing-these can potentially be widely distributed and publicly viewed
- On-line content which is abusive or pornographic

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

As part of the Education Act 2004, the Children's Act, the Every Child Matters agenda and subsequent agendas (including 'Teaching Online Safety in School') set out by the current Government, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of on-line technologies. This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also informs as to how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and

use. The term 'online safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

Whilst the school or setting should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children and young people continue to be protected.
Where possible, another member of staff should be copied into emails to also reduce risks. There is also a responsibility to educate parents about the risks and how this is managed inside school, along with what they can do at home to help safeguard their child.

Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Section 2: Roles and responsibilities of the school:

2.1 Governors and Head Teacher

It is the overall responsibility of the Head Teacher with the Governors to ensure that there is an overview of online safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Head Teacher has designated an Online Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring online safety is addressed in order to establish a safe learning environment. All staff and students are aware of who holds this post within the school.
- Time and resources should be provided for the Online Safety Leader and staff to be trained and update policies, where appropriate.
- The Head Teacher is responsible for promoting online safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Head Teacher should inform the Governors at the Curriculum meetings about the progress of or any updates to the online safety curriculum (via PSHE or Computing) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors are to be made aware of online safety developments from the Curriculum meetings.
- The Governors MUST ensure Child Protection is covered with an awareness of online safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An online safety Governor will challenge the school about having an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using technology, including:
  Challenging the school about having:
  - Anti-virus and anti-spyware software

    - Filters
    - Using an accredited ISP (internet Service Provider)
    - Awareness of wireless technology issues
    - A clear policy on using personal devices.
    - Procedures for misuse, allegations or dealing with e-Safety incidents
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Northamptonshire Safeguarding Children Partnership) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers. See appendices for example procedures on misuse.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Address overuse of blanket e-mails or inappropriate tones

2.2 Online Safety Leader/Computing Co-ordinator

It is the role of the designated Online Safety Leader and the Computing Co-ordinator to:

- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe learning environment within the school.
- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-alone computers, staff/children laptops, children Chromebooks and iPads.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Head Teacher on a regular basis.
- Liaise with the PSHE, Child Protection and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct online safety information can be taught or adhered to.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Northamptonshire Safeguarding Children Partnership (NSCP) to ensure the correct procedures are used with incidents of misuse.
- Ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone computers and teacher laptops and child equipment and that this is reviewed and updated on a regular basis.
- Ensure that the technician can check for viruses on laptops, stand-alone computers and other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised.
- Maintain an e-Safety Incident Log (class teachers to raise matters of concern to online safety lead).
- Ensure teachers know how to log an e-safety incident
- Ensure that the iPad/Laptop user agreement is current, accurate and signed by all pupils and parents before children access their accounts.
- Ensure teachers understand appropriate approvals/usage on Tapestry.

2.3 Staff or adults

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the Designated Person for Child Protection is within school or other setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made

against a member of staff it should be reported immediately to the Head Teacher. In the event of an allegation made against the Head Teacher, the Chair of Governors must be informed immediately. (Following the allegation procedures within the NSCP.)

- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Head Teacher/Safeguarding lead immediately, who should then follow the allegations procedures within the NSCP, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the Online Safety Leader.
- Alert the Online Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with online safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 2018. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in. School bursars will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the Online Safety Leader and school technician in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop when transferring information from the internet on a regular basis, especially when not connected to the school/educational setting's network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.
- Keep usernames and passwords private and never leave work stations unattended when logged in.
- Report accidental access to inappropriate materials to the e-Safety Leader to allow for sites to be added to the restricted list.
- Be mindful of transportation of sensitive pupil/colleague information and photographs on memory sticks, laptops or other devices between school and home. Wherever possible, encryption or password protection should be used to restrict unauthorised access in the event of loss or theft.
- Know the rules contained within the iPad/Laptop user agreement and ensure these are adhered to when carrying out live sessions with pupils or uploading work.
- Know the rules contained within the Tapestry term of service ensure these are adhered to when uploading work-
- Address e-safety incidents regularly throughout the year and ensure that sessions are planned into the curriculum to remind children to the importance of staying safe online. Plan opportunities for children to put their knowledge of e-safety into practice.

2.4 Children and young people

Children and young people should be:

- Involved in the review of the online safety rules through pupil voice in line with this policy being reviewed and updated.
- Responsible for following the online safety rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.

- Taught to use the internet in a safe and responsible manner through Computing, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent) – considering lock it, block it, show it, tell it.
- Aware of the iPad/Laptop agreement and know the rules they need to follow when using the platform.

Section 3: Appropriate and Inappropriate Use:

3.1 By staff or adults

Staff members have access to the network and Google Drive so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access the computer system and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. Staff devices to be locked and password protected when not in use.

All staff will receive a copy of the Acceptable Use Policy and sign to say they have read it. The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the Google Drive and Tapestry from home, the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the event of inappropriate use:

If a member of staff is believed to misuse the internet, or Tapestry in an abusive or illegal manner, a report must be made to the Head Teacher immediately and then the allegations procedures within the NSCP and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

3.2 By Children or Young People

Online safety rules are displayed in all classrooms and the Computing suite. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

Schools or educational settings should encourage parents/carers to support the rules with their child or young person. This can be shown by signing the parent letter with the online safety rules so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school. Parents and children will be responsible for signing the parent letter, online safety rules and Google Classroom user agreement on entry to the school.

The downloading of materials, for example, music files and photographs needs to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using the Google Drive or Tapestry in or beyond school.

In the event of inappropriate use:

Should a child or young person be found to misuse the on-line facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the online safety rules may have their parents contacted explaining the reason for suspending the child or young person's use for a particular lesson or activity. Their Google Drive or Tapestry account can be deactivated for a set period of time if necessary.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and a letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.
- A concern will be recorded on Edukey if appropriate.

In the event that a child or young person accidentally accessed inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. The children follow a slogan 'lock it, block it, show it, tell it' when dealing with inappropriate materials.

Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, (which links to the Online Safety Leader) or KS2 are familiar with the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Section 4: The Curriculum and Tools for Learning:

4.1 Internet use

Schools and educational settings should teach children and young people how to use the internet safely and responsibly. They should also be taught, through computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further their learning. The following concepts, skills and competencies should have been taught by the time they leave Year 6:

- Internet literacy
- Making good judgements about websites and emails received
- Knowledge of risks such as viruses and opening mail from a stranger
- Access to resources that outline how to be safe and responsible when using any on-line technologies
- File-sharing and downloading illegal content

- Uploading information – know what is safe to upload and not upload in terms of personal information
- Where to go for advice and how to report abuse

The Teach Computing scheme of work is used to teach Computing from Year 1 to Year 6. Online safety discussions and activities are embedded throughout each unit of work, as well as being taught as discrete lessons, through the www.thinkuknow.co.uk as well as the project evolve website, throughout the year, particularly on Safer Internet Day.

Online safety skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph)
- Address
- Telephone number
- E-mail address
- School
- Clubs attended and where
- Age or DOB
- Names of parents
- Routes to and from school
- Identifying information, e.g. I am number 8 in the Youth Football Team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Whenever a child uploads a photo or image onto their DB profile, it is sent to the moderator (Online Safety Leader) to be checked. Class teachers will check uploads within their Google Classroom class and Seesaw.

4.2 Pupils with additional learning needs

The school or setting should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

4.3 Learning Platform

Tapestry and the Teach Computing Scheme of work are our providers for our learning platforms and create a wealth of opportunity for adults, children and young people within school to:

- collaborate and share work
- ask questions
- debate issues
- dialogue with peers
- access resources
- develop an on-line community
- receive instant feedback from work

The tools available for use within the learning platform for adults, children and young people include:

- Internet access
- E-mail
- An on-line personal space for adapting as a user to:
    - upload work
    - access calendars and diaries
- Games linked to areas of the curriculum, particularly Maths and English

4.4 Mobile phones and other emerging technologies

Children are not allowed to access or use their mobile phones during the school day. They are stored safely by the office each morning and returned at the end of the day. It is important to consider that increased incidents of bullying and misuse have been reported where students are allowed to use them in school. In settings where clear rules on this issue are agreed to and followed, the level of misuse is reduced. Where inappropriate usage of said technologies does occur a virtual paper trail may be traceable, even if the message received is sent anonymously.

(i) Personal mobile devices and smart technology (including watches)

Staff should be allowed to bring in personal mobile phones or other smart devices (including watches) for their own use, but must not use personal numbers to contact children and young people under any circumstances. The personal devices of employed staff must be kept out of sight at all times and smart watches switched to silent whilst working with children.

Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.

Staff should be aware that games consoles such as the Sony PlayStation, Microsoft Xbox and other such systems have internet access which may not include filtering. Before use within school, authorisation should be sought from the Head Teacher and the activity supervised by a member of staff at all times.

The school is not responsible for any theft, loss or damage of any personal mobile device or other smart technology.

(ii) School/educational establishment issued mobile devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop, iPad, PDA or mobile phone, only this equipment should be used to conduct school business outside of the school environment.
- Agreements should be signed to ensure all equipment is tracked.

4.6 Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to cameras and iPads for photographs and videos.

It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via weblogs, forums or any other means on-line should only occur after permission has been given by a parent/carer or member of staff.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. On the website, photos should always remain anonymous.

Group photographs are preferable to individual children and images of young people should not be of any compromising positions or in inappropriate clothing, e.g. gym kit, swimming costumes.

Photographs of pupils will be stored on the school network system in the staff area. They will be filed in year groups and will be deleted at the end of each school year.
School equipment will be used to take any images of students, and pictures should be removed from cameras/Ipads and utilised appropriately within 24 hours of being taken. This is to ensure that images of students cannot be viewed by unauthorised individuals in the event of loss or theft.

4.5 Video-conferencing and webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult.
Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the online safety rules.

Section 5: Web 2.0 Technologies:

5.1 Managing Social Networking and other Web 2.0 technologies

Social networking sites (including socialising while online gaming) have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service typically offers users both a public and private space through which they can engage with other online users, and express themselves creatively through images, web content and their own personal profile page. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Instagram and TikTok). In response to this issue the following measures should be put in place:

- The school inhibits access to social networking sites through existing filtering systems. Access will only be allowed to Google Drive and Tapestry learning platforms and children are encouraged to communicate through this out of school as well.

- Students are not advised against using any of the social networking sites available, but instead are given advice if they intend to use them to ensure they are using them safely.
- Students are advised against giving out personal details or information which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, and email address or full names of friends.)
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos which could reveal personal details (e.g. house number, street name, school uniform)
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school is aware that social networking can be a vehicle for cyberbullying. Pupils are encouraged to report any incidents of bullying to the school (either directly or by blowing the whistle in the DB learning platform) allowing for the procedures, as set out in the anti-bullying policy, to be followed.

5.2 Social networking advice for staff

Social networking outside of work hours, on non-school issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Head Teacher authorised systems (e.g. Google Drive, Tapestry or TTRS/Spelling Shed for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information. Staff are advised against accepting requests from colleagues until they have checked with them in person that the request is genuine (avoiding fake profiles set up by students).
- Staff are not allowed to accept requests from students or parents at the school.

Section 6: Safeguarding measures:

6.1 Filtering

Staff, children and young people are required to use the Google Drive and Tapestry and all tools within it, in an acceptable way.

The Schools Broadband connectivity has a filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child.

All filtering should be set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet. This also links to the embc-pl criteria 'Schedule 11' of Level Four site filtering to qualify for access to the broadband services.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

The Head Teacher should sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirements from Schools Broadband. In the event that the site level is not set to 'No Access', the Head Teacher and Governors should write a letter to the LA to explain how they intend to safeguard their children and young people.

This complies with the agreed connectivity legalities with Schools Broadband and also ensures our younger audiences are not exposed to unnecessary risks e.g. a blanket Level Two for Primary school users, is inappropriate.

The Google Drive and Tapestry are set within a filtering service that will provide the same level of protection for all users.

Anti-virus and anti-spyware software are used on all network and stand-alone computers or laptops and is updated on a regular basis.

The 'skin' of the on-line personal space is age appropriate and only tools appropriate to the age of the child are available.

Children should use Google as their main search engine, which is highly filtered.

Links or feeds to online safety websites are provided on the website.

KS2 children are familiar with the 'Think you Know' website and the associated 'Report Abuse' button should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and On-line Protection Centre) training for pupils is annual and delivered as part of the Computing curriculum for raising awareness on staying safe and being responsible (using www.thinkuknow.co.uk). The children also take part in Safer Internet Day.

6.2 Tools for bypassing filtering

Web proxies are probably the most popular and successful ways for students to bypass internet filters today, identifying a cause for concern amongst schools and educational settings where children and young people can access the internet. Web proxies provide an anonymous route through filtering safeguards in existence on networked facilities, allowing users to navigate through potentially harmful or inappropriate content. A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which material can be viewed. The most common use of this tool amongst students is to access social networking features, gaming websites or information of an adult nature - all of which is blocked through the school or educational establishment's filtering system.

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school or educational settings security controls (including internet filters, antivirus solutions) as stated in the Acceptable Use Rules.

Violation of this rule should result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

Section 7: Monitoring:

The Online Safety Leader should be monitoring the use of on-line technologies by children and young people and staff, on a regular basis.

Class teachers monitor the use of Google search content, Class logins and Tapestry (where required) for the pupils within their class.

Section 8: Parents:

8.1 Roles

Each child will receive a copy of the online safety rules and iPad/Laptop user agreement on entry to school, which needs to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It will be expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

School will keep a record of the signed forms.

8.2 Support

The school promotes a positive attitude to using the internet and therefore wants parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly.

The school will hold Parent/Carer Information sessions once per annum to deliver key messages and raise awareness for parents/carers and the community. Part of this session will provide parents with information on how the school protects children and young people whilst using the Google Drive, Tapestry and other facilities, such as the internet and e-mail. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible internet users and how this can be extended to use beyond the school environment.

Section 9: Links to other policies:

9.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. Schools/educational settings should have an up to date Anti-bullying Policy which will include any cyberbullying issues.

People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

9.2 Managing allegations and concerns of abuse made against people who work with children.

Please refer to the allegation procedures within the NSCP in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Head teacher within the school or educational setting immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

9.3 Health and Safety

Refer to the Health and Safety Policy and procedures of the school and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

9.4 School website

The uploading of images to the school website should be subject to the same acceptable rules as uploading to any personal on-line space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

9.5 External websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the Head Teacher and unions, using the reporting procedures for monitoring.

Parents, Staff and Pupils agree not to air any grievances about school on social media sites (Facebook/Twitter etc.) but come into school to discuss issues or concerns.

9.6 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Section 10: Staff Procedures Following Misuse by Staff

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by an adult:

A. An inappropriate website is accessed inadvertently:

- Report website to the Online Safety Leader if this is deemed necessary.
- Contact Schools Broadband so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down.
- Log the incident.

- Report to the Head Teacher and Online Safety Leader immediately.
- Head Teacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform relevant authorities.

C. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Head Teacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D. An adult has used computing equipment inappropriately:

- Follow the procedures for B.

E. An adult has communicated with a child or used computing equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Head Teacher and Designated Person for Child Protection immediately, who should then follow the allegations procedures within the NSCP and Child Protection Policy.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Head Teacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Head Teacher or Chair of Governors (if allegation is made against the Head Teacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website, DB learning platform or Google Classroom (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the Head Teacher immediately and follow Child Protection Policy as necessary.
- Inform the LA/NSCP and Online Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Head Teacher.

Section 11: Staff Procedures Following Misuse by Children and Young People

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the Online Safety Leader if this is deemed necessary.
- Contact Schools Broadband and the helpdesk filtering service for school and LA so that it can be added to the banned list or use Local Control to alter within your setting.
- Check the filter level is at the appropriate level for pupil use in school.

B. An inappropriate website is accessed deliberately:

- Refer the child to the online safety rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Inform LA as above.

C. An adult or child has communicated with a child or used IT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Head Teacher and Designated Person for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Head Teacher must follow the allegation procedures within the NSCP and/or Child Protection Policy.
- Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website, DB learning platform or Google Classroom about a child in school:

- Preserve any evidence.
- Inform the Head Teacher immediately.
- Inform the LA/NSCP and online safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Head Teacher immediately.

F. Extreme Incidents:

There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.

They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Procedures need to be followed by the school referring to the allegation procedures within the Northamptonshire Safeguarding Children Partnership.

All adults should know who the Designated Person for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Section 11: Acceptable Use Rules for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or e-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Head Teacher, Designated Person for Child Protection or Online Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school e-mail and phones and only to a child's school e-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Head Teacher and/or Online Safety Leader.
- I know that I should complete virus checks on my laptop or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 2018 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriately requests my password I will check with the Online Safety Leader.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.
- I have been given a copy of the Acceptable Use Policy to refer to about all online safety issues and procedures that I should follow.
- I will follow all rules within the iPad/Laptop (and Tapestry) user agreement.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of online safety and my responsibilities to safeguard children and young people when using on-line technologies.

Name: …….. Role: …….

Signed …….. Date …….....

Section 13: Online Safety Letter to Parents/Carer for Primary

Online Safety Agreement

As the parent or carer of the above pupil, I grant my permission for my child to have access to use of the Internet, school approved e-mail account and other IT facilities at school.

I have read the online safety rules with my child and confirm that he/she has understood what the rules mean.

I accept that ultimately the school cannot be held entirely 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 an educationally filtered service, restricted access e-mail, 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, and that if they have concerns about their online safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet, digital technology and social media at home and will inform the school if I have any concerns over my child's online safety.

Parent/ Guardian name: ……..

Parent/ Guardian signature: ……

I have read the online safety rules with my parent/guardian and I understand the importance of being safe online.

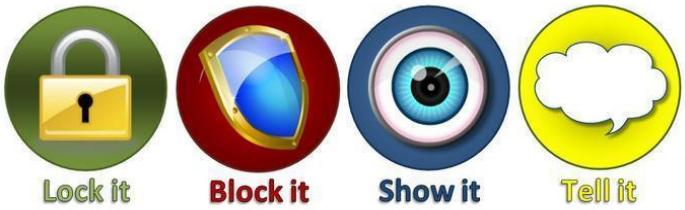
Child's name: ……

Date: ……

Online Safety

I will only use the school's computers for school activities.
I will only edit or delete my own files and not look at, or change, other people's files.
I will not upload files or inappropriate materials or open attachments without permission.
I will ask permission from a member for staff before using the Internet and will not visit Internet sites I know to be banned by the school.
I know how to be responsible when using social network sites.
I will only e-mail people a responsible adult has approved.
The messages I send will always be polite and sensible.
I will not post comments that are unkind or inappropriate about another person online.
I will not give out personal information – such as my name, address, phone number, or e-mail or send photographs or videos to people I don't know and trust.
I will not communicate with someone I do not know online or arrange to meet someone I have only been in touch with online.
I will keep all my login and password details secret.

If I see anything I am unhappy with when I am online, I will tell a responsible adult immediately!



Section 15: Tapestry Parental Consent?

Dear Parents:

I am delighted to share with you that this school year our class will be using Tapestry, a secure online journal where teachers can document and showcase what the children are learning in class. Your teacher will be able to add the things we work on (including photos, videos, worksheets, drawings and voice recordings) to their Tapestry journal and we can share them privately with you and other family members to view and comment on throughout the school year.

In order for your teacher to use Tapestry, the app needs your child's name in order to be able to associate work like their photos, videos or voice recordings with their account. Tapestry only uses this information to provide the service and doesn't advertise in Tapestry, create profiles of students, or share or sell your child's personal information or journal content.

Under an EU law called the General Data Protection Regulation (GDPR), in order for your child to use Tapestry, the school must get your consent. For more information on GDPR, please visit https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens.

I hope that you will enjoy using Tapestry to see all of the learning and activities completed by your child/children throughout the year. Please sign below and return this permission slip so that your teacher can use Tapestry.

————————————————————————————————————

Please sign below and return the form.

I give consent for my child, listed below, to use Tapestry for class activities.

Student Name: _____

Parent Printed Name: _____

Parent Signature: _____ Date: _____

Section 16: Further Information and Guidance:

The nature of online safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

https://www.gov.uk/government/publications/teaching-online-safety-in-schools

http://www.northamptonshirescb.org.uk/ (Northamptonshire Safeguarding Children Board)

www.parentscentre.gov.uk (for parents/carers)

www.ceop.co.uk (for parents/carers and adults)

www.iwf.org.uk (for reporting of illegal images or content)

www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)

www.netsmartzkids.org (5 – 17)

www.kidsmart.org.uk – (all under 11)

www.phonebrain.org.uk (for Yr 5 – 8)

www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)

www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)

www.teachernet.gov.uk (for schools and settings)

www.dcsf.gov.uk (for adults)

www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)

www.becta.org.uk (advice for settings to update policies) and
http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)

www.nen.org.uk (for schools and settings – access to the National Education Network)

https://enable.lpplus.net/ht/online safetyhome (for schools and settings to access online safety guidance and support)