Talavera Junior School
E-safety Policy

Document Name: E-safety Policy

Latest Review: November 2021

Next Review Planned: November 2023

Signed:_____ **(Policy Owner)**

Print Name: Lucy Coombs

Signed:_____ **(Governor Approval)**

Print Name:_____

Approval Date:_____

Talavera Junior School
E-safety Policy

POLICY CHANGE HISTORY

Version	Date	Status	Policy Owner	Governor Approval	Comment
1.0	November 2021		L.Coombs		

Talavera Junior School
E-safety Policy

The E-Safety Policy has been agreed by staff and governors (which included the Designated safeguarding leads) and is based on Hampshire E-Safety guidance.

Rationale

As a school we are confident that internet use enhances educational opportunities, professional development, data management and administration. However, at all times the safety and well-being of our children is the primary concern. This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members. This policy should be read in conjunction with the school's Safeguarding, Whistleblowing, Child Protection, Data Protection, Anti-bullying and Social Media policies and staff acceptable use of ICT policy.

The internet is seen as an integral part of modern day life and is an essential resource in supporting teaching and learning as well as being part of the statutory curriculum. The use of the internet and other digital technologies in school and at home help to stimulate learning, promote discussion and increase awareness of the wider world helping to raise educational standards and promote student achievement. At Talavera Junior we aim to provide children with learning opportunities and experiences which build ICT skills needed to access life-long learning and employment in this rapidly changing world; improving their understanding of doing so in a safe and responsible manner. Through our curriculum we aim to help children begin to be able to evaluate Internet information and begin to take care of their own safety and security both in school and at home.

However, we also understand the use of these new technologies can put young people at risk both within and outside the school setting. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of radicalisation
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / Internet games

- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate these completely. It is therefore essential, through good learning opportunities, to build pupils' resilience to the risks that they may experience, so that they have the confidence and skills to face and deal with them. Talavera must demonstrate that it has provided the necessary safeguarding to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Use of Internet in school

There are many reasons why as a school we choose to use the internet.

- Internet Allows for the teaching of the Computing National Curriculum.
- Access to world-wide educational resources including images and videos.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments and online training courses.
- Access to educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data such as SIMS.
- Access to learning wherever and whenever convenient.
- To promote and celebrate the achievements of the school through a website.

Managing Internet Access in school and across the school system

The school Internet access will be designed expressly for both pupil and staff use and will include filtering appropriate to the age of pupils or job description. In addition to this:

- Pupils will be taught what Internet use is acceptable and what is not and given clear instructions about safe internet usage (see section 'Introducing E-Safety to Pupils').
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for their age group.
- Pupils will be educated in effective ways to search for information online using a range of sources.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Both pupil and staff internet use will be monitored on a regular basis to ensure use of the internet is safe and acceptable.

Evaluating Content on the Internet

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider and reported to the Headteacher and police (when considered appropriate).
- Pupils will be taught to be critically aware of the materials they read and to question its accuracy before accepting it as fact.
- Pupils will be taught how to report unpleasant Internet content through our Online safety lessons (overview of programme included below).

Security of the Network and Online Data and Filtering

At Talavera Junior the Network is overseen by an external company 'Agile' who run regular checks and are in regular communication with the ICT lead. In addition to this, both Agile and the ICT have access to the school's web filtering system which is provided by Hampshire through the Smoothwall web filtering application. To ensure our network and internet use remains safe, the following procedures have been put in place:

- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted, password protected or otherwise secured.
- Pupils are not allowed to download any files or programs without permission from a member of staff.
  Files held on the school's network will be regularly checked.
- Agile, the ICT lead and admin officer will review system capacity regularly.
- Any material that the school believes is illegal or inappropriate must be reported to appropriate agencies such CEOP or the police and will not be opened or edited in any way.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Staff passwords are created by individual staff members and should never be divulged to anyone else.
- Staff laptops are a school resource and staff should exercise caution when downloading files. Staff should consult the head teacher, admin officer or ICT lead before downloading and installing new programs.

School Website Content

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupil's personal information must not be published.
- Only the school admin e-mail should be available on the site.
- Whilst the Senior Leadership Team, the ICT lead and administration staff may edit and add to the school website, The Head teacher will have final approval about website content to ensure it is accurate and appropriate.
- The website will comply with the DfE guidelines for publications including respect for intellectual property rights and copyright.
- Pupil's full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.
- The copyright of all material must be held by the school, or no copyright must be needed. Where permission to reproduce has been obtained, content must be attributed to the owner.

Social Networking

This policy should be read in conjunction with the 'Social Media Policy', where detailed information on social networking is given. Here is some further information for reference:

- Social Networking sites (eg. Facebook, Bebo, MySpace etc) are blocked or filtered on school computers as far as possible.
- Video websites such as Youtube are not blocked on our school computers as it is used by staff as a teaching aid. Pupils will not access video websites such as Youtube themselves at school.
- Pupils will be taught never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, phone numbers, school attended, full names of friends, specific interests and clubs etc.
- Parents will be advised that pupils at Talavera Junior School are too young to have social network accounts and that they should not have access to other people's accounts either.
- Advice should be given regarding details in photographs which are uploaded to social media which could identify a pupil or staff member or his/her location eg. House number, street name or school.
- Parents will be told that any images of their own child on social media must not include the faces of, or information about, any other pupils or staff unless they have the permission of that pupil's parents or the staff member.
- Staff will be advised that they should keep any contact with parents on a professional basis and should not use social networking to contact parents.
- Regular updates regarding social media changes will be provided to parents through our school newsletters and during parent assemblies.
- Staff may have personal social networking accounts, but should be mindful of the content they write, share or upload and understand the privacy settings of their accounts to ensure they do not damage the reputation of themselves or the school. See more in section 13 'School Reputation and Confidentiality', and the section titled 'Cyber Bullying and Harassment of/by Staff and Other Adults'.

Video Conferencing

Video conferencing is a useful tool for staff to communicate with each other and to remotely teach pupils when necessary. When video conferencing with staff or pupils, the following guidelines will be adhered to:

- All videos being shared with pupils will be pre-recorded and watched by a staff member before being shown to pupils, to ensure they are suitable.
- All content being shared with pupils will only be shared with pupils of the appropriate age and maturity. Parental consent will be gained before showing pupils anything rated 'PG' (parental guidance).
- The copyright of all material being shared in video conferencing must be held by the school, or no copyright must be needed. Where permission to reproduce has been obtained, content must be attributed to the owner.
- Staff will be mindful of what can be seen and heard in the background when video conferencing, to make sure images and sounds are appropriate, non-offensive and do not breach individual privacy (eg. full names or addresses on display, images of other people, potentially offensive images etc).
- Staff generally should not share confidential or private information about themselves or others via video conferences. However, if such sharing is required

staff will ensure the video conference is password protected and if the conference is saved, it is encrypted to keep private information safe.

- If a video conference is going to be recorded to be viewed again later, all people in the video conference will be informed before recording begins so that proper consent can be given.
- When screen-sharing during video conferencing, ensure that any documents being used on the computer of a confidential nature are not shown, or are closed prior to beginning screensharing.
- Video conferencing between staff will be accessed using accounts created with staff email addresses (predominately through Google Meet). All Child Protection, Safeguarding, Whistleblowing and Social Media Policies apply when working remotely using video conferencing.

Portable Devices

'Portable devices' includes, but is not limited to, mobile phones, tablets, games consoles, laptop computers, personal organisers, smart watches and internet connected toys. Many of these devices, particularly tablets and laptop computers, have a multitude of different and useful functions and it can be educational to use them in school. Teachers will be able to evaluate their use for a particular function.

- Portable devices will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff mobile phones will generally not be used during lessons or formal school time to make or receive calls/messages.
- Pupils are not permitted to bring their personal portable devices into school (if this becomes a necessity, these will be stored safely in the school office).
- Parents will be reminded that any images taken using portable devices on school property must not include any information which would jeopardise the confidentiality and safety of others (such as pictures including other people's faces, full names or location). Images or recordings of other people may not be taken without their permission.
- All people using portable devices to make phone calls, video calls or to capture photographs and videos will be reminded to be mindful of the background images and sounds, and that others can easily hear what they are saying.
- Games consoles typically will not be used in school. Pupils are not permitted to bring their games consoles into school.

Assessing the Risk

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.

- There are filters in place to ensure content is suitable for children at an age appropriate level
- The ICT lead will run regular safeguarding reports on internet usage of both pupils within the school and staff both within school and when using the school remote server. Results from these reports will be kept securely on file.
- The school will periodically audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Procedures when Concerns are raised

- Inappropriate handing of school IT equipment by pupils will be dealt with in accordance to our school Behaviour Policy.
- Any complaint about staff misuse of equipment or misuse of software or the internet must be referred to the Headteacher. If the complaint is about the Headteacher, it must be referred to the Chair of Governors. See the Whistleblowing Policy for more information.
- Pupils will be encouraged to report any e-safety issues to a parent or guardian when at home or a member of staff when at school.
- Parents can report any areas of concern directly to a child's class teacher which should then in turn be reported to the E-safety Co-Ordinator (Headteacher) and other Designated Safeguarding Lead's if appropriate. Inappropriate behaviour between pupils online outside of school will also be dealt with in accordance to our school Behaviour Policy.

School reputation and confidentiality

The school recognises an employee's right to a private life. However, the school must also ensure its reputation and confidentiality are protected. Therefore, an employee using any ICT away from school, including email and social networking sites must: - - Refrain from identifying themselves as working for the school in a way that could have the effect of bringing the school into disrepute.

- Not express a personal view as a school employee that the school would not want to be associated with.
- Notify a member of SLT immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school.
- Not have any unauthorised contact or accept 'friend' requests through social media with any pupil/student under the age of 18 (including former pupils) unless they are family members.
- Exercise caution when having contact or accepting 'friend' requests through social media with parents so as not to compromise the school's reputation or school information.
- Not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the school and/or partner organisations, pupils/students or parents.
- Not disclose any data or information about the school, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the Data Protection Act 2018.
- Not use the Internet or social media in or outside of work to bully or harass other staff or others. See the section below titled 'Cyber Bullying and Harassment of/by Staff and Other Adults'.

External Use

Any use of school ICT equipment outside of school hours must comply with this policy. Digital equipment provided by the school which is being used by staff at home should be used for work purposes only.

E-Safety (Online safety) Awareness at Talavera Junior School

Teaching of Online safety to pupils

- Each year group will have a dedicated study on online safety (see below titled curriculum overview). This will provide an opportunity for children to extend their understanding of how to be a good online citizen and will provide a platform for discussions on how to stay safe online. This will be taught using age appropriate material, such as CEOPs resources and Project Evolve (government produced resources).
- E-Safety assemblies will take place periodically to remind the children of safe and respectful internet use.
- Each year the school will participate in the National Online Safety week which will provide children with up-to-date learning of key

Introducing E-Safety to Staff

- All staff will have access to the School E-Safety Policy online and its application and importance will be explained.
- Staff should be aware that the school network and internet traffic can be monitored and traced to an individual user. Discretion and professional conduct are essential. Staff cannot expect privacy when using the school's internet facility.
- Certain websites will be blocked, but it is a breach of this guide to access any of the following types of site: - pornography/adult /mature content - gambling/betting - alcohol/tobacco - illegal drugs - violence/hate/racism - weapons - any site engaging in or encouraging illegal activity - illegal file-sharing sites
- Staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the Headteacher or ICT lead. Genuine mistakes and accidents will not be treated as breach of this policy.
- Staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Headteacher.
- Staff must report issues regarding inappropriate material to the ICT lead, which should be filtered or removed immediately.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.
- Staff or adults need to ensure they consider the risks and consequences of anything they may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and the school and can affect future careers.
- Staff members who notice child-protection related issues online will follow the Child Protection Policy procedures and inform the Designated Safeguarding Lead.
- Class teachers will refer interested parents to organisations and websites for further E-Safety information, including CEOPs and the NSPCC. Introducing E-Safety to Parents
- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, during parent assemblies and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

- A partnership approach with parents will be encouraged. This may include: - Parent evenings with demonstrations and suggestions for safe home internet use - Advice on filtering systems - Educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations and websites for further information by Class Teachers, including CEOPs and the NSPCC.

Cyber Bullying, Peer-on-peer abuse and Harassment

Cyber-bullying is defined as 'an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.' By cyber-bullying, we mean:

- Bullying by electronic media.
- Bullying by texts or messages or phone calls.
- The use cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, including blogs, personal websites, social networking sites
- Using e-mail to message upsetting content to others.
- Hijacking/cloning e-mail accounts.
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums including during 'online chats' within gaming apps/ websites.

Cyber Bullying and Harassment of/by Pupils

The school policy for correct procedures regarding a pupil being cyber-bullied is outlined in detail in the school's Safeguarding policy which must be read by all staff.

Cyber Bullying and Harassment of/by Staff and Other Adults

This section should be read in conjunction with the Department of Education guidance contained in "Cyber-bullying: Advice for Headteachers and School Staff". The school will consider it a potential disciplinary matter if staff utilise any information and communications technology, including email and social networking sites, in such a way as to bully or harass others in the school, in professional organisations, pupils or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media site, inappropriate or derogatory information about a colleague, pupil or parents can find its way into the public domain even when not intended. It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment. If a staff member receives any threats, abuse or harassment from members of the public online then they must report such incidents to the Senior Leadership Team, or where necessary the police. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182). The school owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, Youtube or by any other means. If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately

and providing the victim with support which demonstrates that the matter is being dealt with seriously. Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

Curriculum overview

Year 3	Year 4	Year 5	Year 6
How to use online technology safely.	Understand online restrictions and how they keep us safe.	Understand how to be a good online citizen.	Understand how to keep personal information online private.
Understand the benefits and risks of sharing information online.	Understand what makes a good online citizen.	Identify appropriate online friends and the influence they can have on us (begin to discuss mental health).	To consider the impression online photos can give including a focus on mental health.
Identify appropriate online friends.	Understand what cyberbullying is and how to respond appropriately.	Understand the benefits and risks of sharing information online.	Begin to evaluate digital content and understand online risks.
Consider the impressions photos give and how to share responsibly.	Understand how to keep safe when talking to others online.	Identify appropriate and inappropriate online behaviour including the effect it can have.	To understand my digital footprint and its consequence.
Understand what cyberbullying is and how to respond appropriately.	Understand how to share information appropriately online.	Explore the need between a balance in online and offline activity.	Understand the signs and consequences of online bullying and how to deal with them.

L Coombs
Computing lead
July 2021
Review date: September 2021

Signed:_____ (Chair of Governors) Date:_____