



## **Talavera Infant School E-Safety Policy**

The E-Safety Policy has been agreed by staff and governors and is based on Hampshire E-Safety guidance and after considering the 'Teaching Online Safety in Schools' Government guidance last updated in January 2023. The school's E-Safety Co-ordinator is the headteacher who is also the Designated Safeguarding Lead.

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 the young children in our school the primary concern.

This policy applies to the school governing body, all teaching staff 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 any 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 and Social Media policies.

### **1. The Internet in School, Rationale and Entitlement**

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with safe Internet access as part of their learning experience.
- Infant pupils need to be begin to be able to evaluate information from the Internet and begin to take care of their own safety and security.

### **2. Benefits of Using the Internet in School**

- 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 Arbor, SIMS, Teachers2Parents, Tapestry and Purple Mash.
- Access to learning wherever and whenever convenient.
- To promote and celebrate the achievements of the school through a website.
- To allow greater communication between staff and parents through emails, Tapestry and Teachers2Parents.

### **3. Managing Internet Access**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 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.
- Where pupils need to search for information online, they will be instructed in how to do so safely and effectively.
- Internet usage by pupils at school will always be supervised by a member of staff.
- Parents will be informed that pupils will be provided with supervised Internet access.

### **4. 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 Harrap, who can block the website, and reported to the headteacher.
- Pupils should be taught to be critically aware of the materials they read and to question their accuracy before accepting it as fact.
- Pupils will be taught how to report unpleasant Internet content through our Internet Safety lessons in the Autumn Term each year.

### **5. Management of Email**

- Staff email accounts can only be set-up by the network manager / admin officer with permission from the headteacher.
- Staff email accounts will only be used for work-related emails.
- Staff must not create, download, upload or transmit any unsolicited commercial or bulk web mail, chain letters or advertisements.
- Pupils at Talavera Infant School will not have school email addresses.
- In the unlikely circumstance that pupils have private email addresses and is it necessary to open an email at school, they will do so only if supervised by a member of staff.
- E-mails sent to an external organisation should be written carefully and sent using work email addresses. Emails to external organisations should be approved by the relevant leaders (eg. subject leader, year leader, SENCO, Deputy headteacher or headteacher).

### **6. Security of the Network and Online Data**

- 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.
- The Computing Subject Leader and admin officer will review system capacity regularly.
- Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP or the police.
- 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 and iPads are a school resource and staff should exercise caution when downloading files. Staff should consult the headteacher, admin officer or network manager before downloading and installing new programs.

## **7. 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 or the headteacher's work email address should be available on the site.
- Whilst the Senior Leadership Team, the Computing Subject Leader and administration staff may edit and add to the school website, The Headteacher will have final approval about website content to ensure it is accurate and appropriate.
- 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.

## **8. 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 and iPads 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 their real name, address, phone numbers, school attended, full names of friends, specific interests and clubs etc.
- Parents will be advised via a Newsletter that pupils at Talavera Infant School are too young to have social network accounts and that they should not have access to other people's accounts either.
- The school will not post pictures of pupils to social media without explicit parental consent. Caution is advised 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.
- 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 of this policy 'School Reputation and Confidentiality', and the section titled 'Cyber Bullying and Harassment of/by Staff and Other Adults'.

## **9. 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 pre-recorded videos being shared with pupils will be watched by a staff member before being shared, to ensure they are suitable.
- All video 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.
- When remotely teaching pupils, staff will be mindful of what can be seen and heard in the background to make sure all images and sounds are age-appropriate, non-offensive and do not breach individual privacy (eg. full names or addresses on display, images of other people, potentially offensive images etc).
- When remotely teaching pupils, the headteacher or a member of the senior management team will be made aware that a remote session with children is happening ahead of time, including details such as why it is happening, who is being invited to the remote session and the nature of what will be taught or discussed.
- 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 screen-sharing.
- All work-related video conferencing between staff will be accessed using accounts created with staff email addresses, not through personal social media accounts. All Child Protection, Safeguarding, Whistleblowing and Social Media Policies apply when working remotely using video conferencing.

## **10. Portable Devices**

'Potable 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 members' personal 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.
- 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.

## **11. 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 infant school level.
- 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.

## **12. 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) or other Designated Safeguarding Leads.

## **13. 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 the E-Safety Co-Ordinator 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' or 'follow' 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' or 'follow' 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'.

#### **14. 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.

### **Filtering and Monitoring at Talavera Infant School**

#### **The Role of the Designated Safeguarding Lead**

The Designated Safeguarding Lead (in this case the headteacher) is responsible for safeguarding and online safety which includes:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of the provision provided
- overseeing and acting upon reports
- overseeing and acting upon safeguarding concerns
- overseeing and acting upon checks to filtering and monitoring systems

The Designated Safeguarding Lead must also ensure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

## **The Role of All Staff**

All staff are responsible for reporting to the Designated Safeguarding Lead whenever they:

- witness or suspect unsuitable material has been accessed
- access unsuitable material
- are teaching topics that could create unusual activity on the filtering logs
- find there is failure in the software or abuse of the system
- think there are some unreasonable restrictions that affect teaching and learning or administrative tasks
- notice abbreviations or misspellings that allow access to restricted material

All staff have been trained and know that they should report their concerns around filtering and monitoring to the designated safeguarding lead as soon as practically possible.

## **The Role of the IT Service Provider**

The IT provider for Talavera Infant School has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and designated safeguarding lead to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

## **How Filtering and Monitoring works at Talavera Infant School**

We use Watchguard for our filtering. This involves a physical box at the school which all network traffic passes through to reach the internet.

This means no matter what the device, as soon as it connects to the school network the device will be filtered in some capacity.

Devices have a certificate installed on them, allowing the Watchguard filtering to inspect traffic on HTTPS sites further. This allows more advanced filtering over pure DNS filtering.

Devices that are connected to the school's Windows domain (Windows PCs & Laptops) will have filtering based on the user's Windows login. If a user logs in with staff credentials they will have access to the staff-level filtering. If a user logs in with student credentials they will have student-level filtering.

Devices not connected to the domain, such as home laptops, mobile phones, iPads & Chromebooks will be seen as an 'unauthenticated device'. These devices will receive the 'Unauthenticated' filtering

provision. By default, this is very locked down in a similar way to the 'Student' filtering, but it may have fewer restrictions if requested by the school.

The filtering is based on categories provided and updated by the IWF (Internet Watch Foundation). The categories and further details can be found in this document - [Harrap Internet - Web Filtering Categories](#)

The above link highlights what we block as default at Talavera Infant School along with some definitions regarding what to expect to be covered in each of the categories.

## **E-Safety Awareness at Talavera Infant School**

### **Introducing E-safety to Pupils**

- In the Autumn Term, Internet Safety will be the first computing subject taught in KS1 classrooms, so that pupils are aware of how to stay safe before using the internet and other software. E-Safety rules will then be embedded with pupils each time they are going to access the internet at school and these 'refreshers' of internet safety information will be part of the planning. This will be taught using infant-accessible material, such as CEOP and thinkuknow.co.uk.
- E-Safety assemblies will take place periodically to remind the children of safe and respectful internet use.
- E-Safety rules will be displayed in rooms with Internet access that the children use.
- The school will participate in Safer Internet Day every year with an assembly and appropriate classroom activities organised by the Computing Curriculum Leader.

### **Introducing E-Safety to Staff**

- All staff will have access to the School E-Safety Policy 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. 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 E-Safety Co-Ordinator (headteacher), which should be filtered or removed immediately.
- All teaching staff will complete online safety training and sign the Acceptable Use of ICT policy at induction.
- 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.

### **Introducing E-Safety to Parents**

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, and on the school website.
- Half-Termly newsletters will be sent to parents with covering a wide variety of E-Safety topics to help parents keep their children safe online at home.
- Internet issues will be handled sensitively by staff, 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 and half-termly Newsletters, including CEOP and thinkuknow.

### **Cyber Bullying 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 via electronic media.
- Bullying via 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.

### **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.

In instances where a pupil is cyber bullying another pupil, the schools Behaviour Policy and Safeguarding Policy will be adhered to.

Staff will assure the pupils know that we expect the same standards of behaviour whenever a pupil is online as we do when they are offline.

### **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 Assistance Programme (0800 028 0199 / <https://healthassuredeap.co.uk/home/>).

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. If staff have reason to

believe a device contains indecent images of children, they must not look at the content. The evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it and then the police should be contacted immediately for advice.

|                   |                       |
|-------------------|-----------------------|
| Responsibility:   | Children and Learning |
| Review cycle:     | 3 years               |
| Date Agreed:      | November 2023         |
| Next Review Date: | November 2026         |