Writtle Infant School

A very special place, where learning has no limits.

Internet Access/E-safety Policy

Date of policy:	March 2014
Date last review adopted by governing body:	10th March 2022
Frequency of review:	Annual

1. Introduction

This document is a statement of the aims, principles and strategies with regard to Internet use at Writtle Infant School. Creating a safe ICT learning environment must include the following:

- An infrastructure of whole-school awareness, designated responsibilities, policies and procedures.
- An effective range of technological tools.
- A comprehensive E-safety education programme for the whole school community.
- A review process which continually monitors the effectiveness of the above.
- Ensure that children are safe from terrorist and extremist material when accessing the internet in school

This policy should be seen as a partner to our Child Protection policy which details how the school deals with on-line issues such as sexting. The Child Protection officer (The Headteacher – Helen Castell) and the Deputy Child Protection Officer (The Deputy Head – Tracey Wilson) are responsible for online E-safety. Staff are to report any online concerns to the relevant staff and also parents will be reminded of this in newsletters and on our website.

Please see in conjunction with our Communications Policy.

The expectations of staff in terms of internet use/ social networking etc. is covered by our Code of Conduct policy and this policy should also be read in conjunction with the Data Protection Policy which also covers GDPR regulations

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments

- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. While at this age group we would not expect any children to be involved with social networking etc., any cases will be dealt with in the same way as Safeguarding issues.

At Writtle Infant School we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We have a planned online E-safety education programme, using discrete lessons, formal lessons and wider curriculum opportunities.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

2. Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Essex County Council (ECC) staff.

3. Aims

- To enable all children to access the internet safely.
- To maximise and access resources to improve a wide range of areas within school.
- To enable staff and our school to communicate more effectively with children, parents, other members of our school and the local community.
- To ensure we are working within the DfE guidance 2019 Keeping Safe in Education which states that:

- "Governing bodies should ensure there are appropriate procedures in place to safeguard and promote children's welfare….which should include acceptable use of technologies and communications including the use of social media."

4. Online-Bullying

Any cases of online-bullying will be acted upon in accordance with our Anti-bullying policy. Children are given lessons on what to do and parents are given advice on how to deal with this.

5. Safeguarding

- To access worldwide resources safely, recognising potential risks.
- The school computers have a filtering system in place which accesses the internet, to enable inappropriate sites to be blocked.
- Children use the internet with supervision and for the screen to be visible to the adult.

6. Strategies for responsible internet use

- E-safety is embedded in all computing lessons to ensure children are aware at all times
- Memory sticks or CDs from outside school cannot be used in school computers.
- Staff guide children in on-line activities that will support the learning outcomes appropriate to the child's age and maturity.
- Permission from a teacher is needed before accessing the internet.
- Permission from a teacher is needed before checking for email.
- Staff are informed of recent updates related to internet use in relation to the curriculum
- The ICT co-ordinator and Headteacher should be informed of any inappropriate material found whilst using the computer in order to block access. The URL and content must be reported to the internet service provider via the ICT co-ordinator or Headteacher.
- The school works in partnership with parents, the LA, DFE and the internet service provider to ensure systems to protect children are reviewed and improved when needed.
- All staff will be provided with the Code of Conduct policy.
- All parents are provided with information about Internet Safety through a dedicated area on our website, leaflets and meetings. This includes how to make internet access safe at home. Frequent reminders are on our school newsletters.
- Details of ALL E-safety incidents to be recorded by the Headteacher. Any incidents are reported to the governors termly
- We have a clear security strategy including network identification for all users, regular changing of passwords, anti-virus prevention is applied, systems backup and clear routines for managing security incidents (via Essex)
- We will discuss with parents any concerns re safe internet use, for example if we discover a child has a Youtube presence as per our Child Protection policy.
- Staff to use hangouts for internal communication

7. Writtle Infant School website

Our school website can be found at www.writtleinfantschool.com. Children's work is included where appropriate and is subject to parental permission, which is requested on the school admission form. Strict rules apply for protecting children's privacy and names are not used. Other areas of the website are monitored by the office staff and Headteacher and any adjustment or information is undertaken by our office manager.

8. Writtle Infant School ParentMail/Tapestry

The school uses ParentMail which is a broadcast communication tool used for large scale communications by text message or email. Up to date information can then be sent to groups of parents who have signed up for this service. Tapestry is used as the online learning journal in EYFS and updated regularly.

9. Data protection

Any item that can hold computer information is classed as media. This includes hard drives, CDs, DVDs, printed output, tapes and memory sticks. Modern media is easy to move so requires extra controls to ensure it is not damaged, stolen or accessed by unauthorised people. Staff are aware of this and put in place measures to reduce these risks where possible, such as ensuring that CDs, DVDs and memory sticks are stored in appropriate places. Permission is given by parents concerning their child being photographed within and outside school and is outlined in our 'Policy on photography in school'. The use of digital cameras means that children's photographs may be used for a variety of purposes including recording achievements and providing evidence for standards. Children and parents are given training on the use of passwords and what to do when we see unfiltered images.

10. Staff email use

Emails sent or received by the school are sent via the school's office, the email address for this is admin@writtleinfantschool.com. The Headteacher also has her own email address. Parents can also contact the school and be contacted on parents@writtleinfantschool.com.

11. Prevent

From 1 July 2015 specified authorities, including all schools as defined in the summary of this guidance, are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 ("the CTSA 2015"), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism" This duty is known as the Prevent duty.

The statutory Prevent guidance summarises the requirements on schools in terms of four general themes: risk assessment, working in partnership, staff training and IT policies. Schools are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This means being able to demonstrate both a general understanding of the risks affecting children and young people in the area and a specific understanding of how to identify individual children who may be at risk of radicalisation and what to do to support them. Schools and

colleges should have clear procedures in place for protecting children at risk of radicalisation. These procedures will follow existing safeguarding policies.

12.Video Conferencing

Video conference meetings shall be subject to the same rules and codes as regular Governing Body meetings and staff meetings. To maximise privacy and safety, the following procedures shall be adopted when using video calling services, which could have potential security issues.

- Enforce encryption by default and make sure it is end-to-end if possible.
- Lock and password protect meetings.
- Unauthenticated users should be held in a waiting room so the organiser can check their identity before admitting them to the call.
- Make sure the meeting host monitors the participant's list and ensures no unknown participant joins.
- Be careful with meeting recordings and get consent from the participants.
- Be aware that audio-only participants calling via a regular phone dial-in option will "break" the encryption.
- Be careful with file and screen-sharing capabilities. They could accidentally disclose sensitive information or be used to spread malicious programmes.
- Be aware video conferencing may be recorded, inappropriate comments should be avoided.

13. Role of Governors

Governors determine, support, monitor and review the school policies. They support the use of appropriate teaching strategies by allocating resources effectively. They ensure that the building and equipment are safe. They monitor pupil attainment across the school and ensure that staff development and performance management promote good quality teaching.

14. Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

15. Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

16. Equality Statement

The governors and staff are committed to providing the full range of opportunities for all pupils regardless of gender, disability, and ethnicity, social, cultural or religious background. All pupils have access to the curriculum and the right to a learning environment which dispels ignorance, prejudice or stereotyping.