E-Safety Policy
Wincle CE Primary School

Version: APPROVED

Updated: March 2021

Wincle CE Primary School
Wincle
Macclesfield
Cheshire
SK11 0QH
Tel: 01260 387 387
Headteacher: Mrs S Smith
Chair of Governors: Dr J Miller

Our school’s vision:

Wincle School creates an enriching and outstanding rural education, nurturing the whole individual: body, mind and soul, inspiring rounded, happy, courageous children who exhibit a passion for learning, a confident faith, a loving concern for community and an inclusive respect for all.

We encourage our pupils to ‘Shine like Stars’ (Philippians 2:15) and to do this run with the following acronym:

S	**Service**	☆ No act of kindness, no matter how small, is ever wasted.” Aesop ☆ We would like our pupils to have the confidence to know that they can make a difference: have hope for the future. ☆ We encourage our pupils to challenge injustice and inequality
T	**Theology**	☆ Our principles are founded on the truth that we are loved by the Father, Saved by the Son and Sanctified by the Holy Spirit. ☆ We want to ignite passion and curiosity for learning, providing an exciting curriculum to inspire all learners to be the best they can be.
A	**Attitude**	☆ We encourage our pupils to show integrity ☆ We would like our pupils to have the courage to fight for what is important ☆ When things are challenging, we would like our pupils to display perseverance and not give up. ☆ Learn from yesterday, live for today, hope for tomorrow” Albert Einstein
R	**Relationships**	☆ We nurture the whole individual: body, mind and soul ☆ We encourage the pupils to respect every living creature and show compassion. ☆ We would like our children to treat other people as they would like to be treated following Jesus’ example. We are all unique ☆ We help all children build trusting relationships ☆ ☆ Clothe yourselves with compassion, kindness, humility, gentleness and patience.’ (Colossians 3:12)
S	**Shine like stars**	☆ "I am the Light of the world; he who follows Me will not walk in the darkness, but will have the Light of life." (John 8:12) ☆ We would like our pupils to shine in their behaviour, attitudes, relationships and learning.

E Safety Policy

1. Introduction

Wincle CE Primary School understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst Wincle CE Primary School recognises the importance of promoting the use of computer technology throughout the curriculum, it also recognises the need for safe internet access and appropriate use. Wincle CE Primary School has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. This school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

2. Using the Internet for Learning in Academies

All pupils are taught how to find appropriate information on the internet and how to ensure as far as possible, that they understand who has made this information available and how accurate and truthful it is. Teachers carefully plan all internet-based teaching and lessons to ensure that pupils are focused and using appropriate and relevant materials. Children are taught how to use search engines and how to evaluate internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary. They are taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils in Key Stage 1 will not be permitted to ‘free-surf’ the web. In Key Stage 1 and typically in Key Stage 2, pupils’ internet access will be through a selection of evaluated sites suitable for the purposes of the task. Processes are in place for dealing with any unsuitable material that is found during internet use. Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit. Pupils who need to search individually will be in the upper primary years. Teachers, wherever possible, will have viewed the content prior to use to check its relevance and suitability. The school's internet access includes filtering appropriate to the age of the pupils which is provided by an approved supplier.

3. Evaluating Internet Content

The school will ensure that staff and pupils are mindful of copyright regulations when copying, downloading and representing materials from the internet. Web-based resources have similar copyright status to printed and recorded materials, such as books, films and music, and this must be taken into consideration when using them. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work. Pupils, during Key Stage 2, will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught how to carry out simple checks for bias and misinformation.

4. Internet Use by Staff

Wincle CE Primary School understands that the internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that we can use to support and enhance learning. It allows staff to share resources with other academies, and to engage in debate and discussion on educational topics and news. It also provides an efficient way to access information from the Department for Education and other government agencies and departments that will help staff to keep abreast of national and local developments. There are also increasing opportunities for staff to access INSET and Continuing Professional Development activities using the Internet and e-learning resources.

Wincle CE Primary School is committed to encouraging and supporting school staff to make the best use of ICT and all the opportunities it offers to enhance our teaching and support learning. Staff use of the internet on school computers will be responsible and legal at all times and in keeping with their professional role and responsibility. Misuse of the internet and school computer systems will be rigorously investigated and could lead to disciplinary action being taken.

5. E-mail

E-mail is one of the many modes of communication which plays an important role in many aspects of our lives today. The school teaches the use of e-mail as part of the Computing curriculum to educate children to be aware of the benefits and risks and how to be safe and responsible users as part of e-safety provision. Pupils are taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly, not including any unsuitable or abusive material. Pupils are taught not to reveal personal details of themselves or others in e-mail communication, nor to arrange to meet anyone without specific permission. Staff must use the school email service and accounts that are available for professional communication. They are more secure and are easier to access by a third party should the need for scrutiny arise. Staff should always ensure that they represent the school in a professional and appropriate way when sending e-mail, contributing to online discussions or posting to public websites. Failure to do so could lead to disciplinary action being taken.

6. Published Content and the School Website

The contact details on the school web site will be the school address, e-mail and telephone number. Individual personal contact information will not be published. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. It will be the responsibility of other staff, personally or by delegation to update the website regularly.

7. Publishing Pupils' Images and Work

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images and video that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images / video on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school/will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm. Staff are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images which states that:

• Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute or danger;

• Nobody should take, use, share, publish or distribute images of others without their permission;

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;

• Pupils' full names will not be used anywhere on the website or learning platform, particularly in association with photographs;

• Parents or carers are informed of our policy on publishing and are able to opt their children out.

8. Communication Technologies – Including Chat, Forums, Blogs, Instant Messenger Services, Social Networking Sites

Most of these modes of electronic communication are restricted in the school however they are being used more frequently by pupils and staff outside of the school. We acknowledge social networking sites, blogs, instant messenger services, chat rooms and forums are beneficial for communication, learning and research. They also present a range of personal safety and privacy issues.

In school time, pupils and staff are not permitted to access social networking sites, public chat rooms, discussion groups and forums etc. using school resources. Most are blocked by the filtering service used by the school.

9. Mobile Phones and Other Handheld Devices (Including those that are Internet Enabled)

It is anticipated that more pupils will have access to internet-enabled devices such as mobile phones or other hand-held devices which are capable of browsing and uploading to the internet, accessing email and social networking services, as well as taking photos and recording video. The school recognises the potential advantages these devices can offer for staff and pupils and there are clear and enforceable rules for their use. Pupils are taught the legal and moral implications of posting photos and personal information from mobile phones to public websites and how to use these technologies in a safe and responsible manner. Children must not bring mobile phones to the school. Only in exceptional, prior arranged circumstances will the school permit mobile phones belonging to pupils on the school premises. If such a set of circumstances is deemed necessary, the mobile phone will be kept securely by the pupil's class teacher. Staff should represent the school in a professional and appropriate way when communicating via the internet, contributing to online discussions or posting to public websites using Academy facilities.

10. Electronic Communications with Children by Staff
Communication between children and school staff should take place within clear and explicit professional boundaries. Staff must be careful not to share any personal information with children such as email, web based communication facilities, home or mobile numbers. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role. Staff should ensure that all communications are transparent and open to scrutiny. In addition, all staff must be sure of their social networking and uphold professional confidentiality at all times.

11. Downloads
Pupils must not be allowed to download any material from the internet on to school computers unless directed to do so by an appropriate staff member. Staff should take care that files from both other computers outside the school and internet are checked for virus contamination before they are used on the school system. Pupils are not allowed to use CDs, DVDs or memory sticks brought from home unless they have been given permission. The school subscribes to suitable antivirus software. The software is updated regularly.

12. Managing Filtering
Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

- Making a note of the website and any other websites linked to it;
- Informing the headteacher
- Logging the incident;
- Informing the Internet Service Provider so that the website can be added to the content filter if appropriate;
- Discussion with the pupil about the incident, and how they might avoid similar experiences in future
- Parents will be informed where necessary. Pupils or staff who deliberately try and access unsuitable materials will be dealt with in accordance with the school's discipline policies for pupils and staff.

13. Managing Emerging Technologies, Video-Conferencing and Electronic Resources for Learning Emerging technologies and resources will be examined for educational benefit and a risk assessment will be carried out before use in the school is permitted.

14. Online Bullying and Harassment (Cyberbullying)
Online bullying and harassment via Instant messaging, chat rooms, social networking sites etc. are potential problems that can have an effect on the wellbeing of pupils and staff alike. There are a range of strategies and policies in place to prevent online bullying. These include:

- No access in the school to public chat-rooms, instant messaging services and social networking sites;
- Pupils are taught how to use the internet safely and responsibly which includes how to identify and respond to 'cyberbullying';
- Children are taught how and where to report incidents that make them feel unhappy or worried;
- As with any form of bullying, pupils are encouraged to discuss with staff any concerns or worries they have about online bullying and harassment.

15. Authorising Internet Access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents are asked to sign and return a consent form when their child starts at the school.

16. Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can't accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision (including system and security) regularly to establish if the E-safety policy is adequate and that its implementation is effective.

17. Handling E-Safety Complaints

Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with the child protection procedures. Pupils and parents will be informed of the complaint's procedure.

18. Introducing the E-Safety Policy to Pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use can be monitored. Pupils will create a code of conduct with their new teachers which will reference E-Safety.

19. Staff and the E-Safety policy

All staff will be given access to the school E-Safety Policy and its importance will be explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

20. Parental Support

Some parents and carers might have a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school provides information and awareness to parents and carers through:

- Information in newsletters;
- Links to resources from the website;
- Parent workshops.

21. Governing Body

GB members should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / E-safety/ health and safety / safeguarding. They should also sign the Acceptable Use Agreement.

Appendix 1 - Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in the school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not sign up to online services until I am old enough

Dear Parent/ Carer,

ICT, including the internet, email and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Smith.
Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

∀ **Parent/ carer signature**

We have discussed this document with ……………………………………………(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Wincle CE Primary School.

Parent/ Carer Signature …………………………………………………

Class ………………………………… Date ………………………………

Appendix 2 - Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the headteacher.
- I will not install any hardware or software without the permission of the headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community without the permission of the headteacher
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or the headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in the school and outside the school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ………………………………………………………………… Date ……………………
Full Name ……………………………………………………………….... (printed)
Job title ……………………………………………………………………

Social Media Policy

This policy is applicable to all employees of Wincle Primary School and covers all uses of social networking applications which are used privately.

This policy should be read alongside our Disciplinary Policy and Procedure, , Acceptable Use Policy and ICT Security Policies and Procedures.

AIMS

To support all employees by establishing clear guidelines on the proper use of social media so that:

- the school is not exposed to legal challenge;
- the reputation of the school is not adversely affected;
- employees do not put themselves in a vulnerable position;
- employees understand how information provided via social networking applications can be representative of the school; and
- the use of social media does not impact on the school.

PRINCIPLES

The school recognises that many employees make use of social media in a personal capacity and, in the majority of cases, this is uncomplicated and trouble-free. Whilst the school respects an employee's right to a private life and has no wish to interfere with this, when using such sites employees must consider the potential impact it could have on their professional position, their own reputation and that of the school. The following identifies how an employee's personal life and work life can start to overlap.

- By identifying themselves as employees of the school, i.e. adding the school name on profiles, the perception of users will be that staff are representative of the school. It is therefore important that employees are mindful of the professional standards that are expected of them. Anything posted, including innocent remarks, have the potential to escalate into something that could potentially damage the image and reputation of the school or Council, or undermine its work. The originating comment may be traced back to an employee of the school and, even if they have not been involved in the latter stages of the comments, they may find themselves subject to a disciplinary investigation.

- Individuals making complaints search the web for information about staff involved in their case – finding social networking sites, blogs and photo galleries that could give fuel to their concerns or help them to identify personal information about them.

- Journalists increasingly use the web to research stories, and may reprint photos or comments that they find.

- Law firms research social networking sites as a matter of course in preparing divorce, private law children's cases and other court proceedings.

- Some organisations also look on social networking sites to find out information about people applying for jobs.

SOCIAL MEDIA

Definition of social media

For the purpose of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. The term social media refers to a number of online networking platforms such as:

- blogs (written, video, podcasts), e.g. WordPress, Blogger, Tumblr;
- micro-blogging websites, e.g. Twitter;
- social networks, e.g. Facebook, LinkedIn;
- forums/message boards; and
- content-sharing sites, e.g. Flickr, YouTube and Instagram.

Employees should be aware that there are many more examples of social media and this is a constantly changing area. Employees should follow the guidelines outlined in this policy in relation to any social media that they use.

Personal use of social media at work

Employees are not allowed to access social media websites for their personal use from the school's computers or devices at any time. This includes laptop/palm-top/hand-held computers or devices (e.g. mobile phones) distributed by the school for work purposes.

The school understands that employees may wish to use their own computers or devices, such as laptops and palm-top and hand-held devices (e.g. mobile phones), to access social media websites while they are at work. Employees must limit their personal use of social media on their own equipment to their official rest breaks such as on their lunch break/times. The use of any personal computers or devices must be discreet, appropriate (e.g. not in the presence of pupils) and in no way interfere with work.

Mobile phones, should always be switched off and left in a safe place during lesson times.

Social media in a personal capacity

The school recognises that many employees make use of social media in a personal capacity. However, the employee's online profile, e.g. the name of a blog or a Twitter name, must not contain the school name. Furthermore, while they are not acting on behalf of the school, employees must be aware that they can damage the school if they are recognised as being one of the school employees. Any communications that employees make in a personal capacity through social media must not:

a. bring the school into disrepute, for example by:
   - criticising the school;
   - criticising or arguing with management, colleagues, children or their families;
   - making defamatory comments about individuals or other organisations; or
   - posting images that are inappropriate, for example, photographs of themselves or colleagues taken at work or links to inappropriate content;

b. breach confidentiality, for example by:

- revealing any information owned by the school; or
- giving away confidential information about an individual (such as a colleague or child) or an organisation, e.g. the school or the Local Authority;

c. abuse their position of trust when working with children/young people, for example by:
    - contacting children or their families through social networking sites unless the reason for this contact has been clearly and firmly established by the head teacher, principal or chair of governors;
    - accepting any requests to become a named friend on a social networking site made by a child/young person; or
    - uploading any photographs or video containing images of children/young people for whom the employee holds a position of trust unless in line with the school procedures;

d. breach copyright, for example by:
    - using someone else's images or written content without permission;
    - failing to give acknowledgement where permission has been given to reproduce something; or

e. do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual (such as an employee of the school);
    - using social media to exclude other individuals; or
    - posting images that are discriminatory or offensive.

Security and identity theft

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private. Employees should never send abusive or defamatory messages.

Employees must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:

- ensure that no information is made available, or referred to, that could provide a person with unauthorised access to the school and/or any confidential information;
- inform their manager immediately if they suspect that their personal site has been compromised or accessed by an unauthorised person;
- refrain from recording any confidential information regarding the school on any social networking website;
- check their security settings on social networking site so that information is only visible to the people who they want to see it;
- put their name into an internet search engine to see what people can find out about them; and
- help friends and colleagues out by letting them know if they spot things on their pages that might be misconstrued.

Defamatory statements

Material posted on a site may be defamatory if it contains something about the school's employees, partners, children or other individuals that an employee may come into contact with during the course of their work that is not true and undermines the school's reputation. For example, photographs or cartoons that may have been doctored to associate the school or its employees with a discreditable act.

Libellous statements

Material posted on a site may be considered libellous if it is in permanent form and directly or indirectly clearly identifies the school or one of its employees or children with material that damages their reputation. Employees should always use their own judgment but should bear in mind:

- that information that they share through social networking sites is still subject to copyright, Data Protection, Freedom of Information and Safeguarding legislation;
- the Code of Conduct; and
- other relevant school policies (e.g. Whistleblowing Procedure, Equality Policy and policies and guidance regarding acceptable use of email, intranet and internet whilst at work).

DISCIPLINARY ACTION

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action under the school's disciplinary procedure. In situations where it becomes known that an employee has posted material to be defamatory or a breach of contract, the employee will be asked to remove the offending material from the social media site immediately.

Serious breaches of this policy, e.g. incidents of bullying of colleagues or social media activity causing serious damage to the school, may constitute gross misconduct and could result in dismissal.

EQUALITY

Wincle CE Primary School will ensure that, when implementing the Social Media Policy, no employee will be disadvantaged on the basis of their gender or transgender, marital status or civil partnership, racial group, religion or belief, sexual orientation, age, disability, pregnancy or maternity, social or economic status or caring responsibility. This means that the policy may need to be adjusted to cater for the specific needs of an individual including the provision of information in alternative formats where necessary.