E-SAFETY AND ACCEPTABLE USE POLICY

Name of School:	Winthorpe Primary School
Date of Policy:	November 2024
Responsibility of:	Governors
Review Date:	November 2026

The computer systems within school are made available to students, staff, and other adults to further their education and to enhance professional activities including teaching, administration, and management.

Safeguarding is a serious matter; at Winthorpe Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, E-safety, is an area that is constantly evolving and as such this policy will be reviewed regularly or in response to an e-safety incident.

The purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.
- To protect all parties – the students, the staff, other adults and the school

This policy is available for anybody to read on the Winthorpe Primary School website; upon review all members of staff will sign as read and understood.

The Family School Code and Acceptable Use Permission form will be sent home with students at the beginning of each school year. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy biannually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of Innovation at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the Innovation Lead, as indicated below.
The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Innovation Lead has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

Innovation Lead

The Innovation Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with ICT Technical Support.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age
    - The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the Headteacher (and an e-Safety Incident report is made).

All Students

The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Permission form; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through school newsletters, the school will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Permission Form before any access can be granted to school ICT equipment or services.

Technology

Winthorpe Primary School uses a range of devices including PC's, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Webfilter software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Innovation Lead, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Webfilter software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords – all staff will be unable to access PC's and laptops without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise. The Innovation Lead and IT Support will be responsible for reminding staff to change passwords.

Class Passwords – Each class has one log on username and password for PC's and laptops. Children are made aware of the username and password at the start of the year. The innovation lead is responsible for changing the class password on a termly basis. Children are shown how to log on using their class username and password at the start of each school year. Teachers must use classroom monitoring software Securly to monitor all computer use. Securly is stored on staff laptops and teachers have the ability to watch student live laptop screen during lessons. Teachers can check the browsing history of their students that occurred during class, while administrators can view all the history of all students.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Biometric data – Our staff Apple devices use fingerprint recognition. This is not used or stored anywhere apart from the device allocated to the individual member of staff. Staff know that the use of fingerprint recognition is optional. Apple devices are also passcode protected.

Safe Use

We promote E-Safety with the 'Think then Click' safeguarding guidelines. These are taught and are on display throughout the school.

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this policy; students upon signing and returning their acceptance of the Family School Code.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Family School Code and the Acceptable Use permission form

Social Networking – there are many social networking services available; Winthorpe Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Winthorpe Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- X (Previously Twitter)

In addition, the following is to be strictly adhered to:

- Permission forms must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Winthorpe Primary School will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Innovation Lead is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use

Staff must always log in using their individual log in and log out appropriately they have finished using the machine.

Passwords should be changed regularly and not revealed to anyone else unless there are exceptional circumstances. Staff and students should never attempt to log onto the system as another student or member of staff in any circumstance.

Any files stored on the 'Staffroom' drive will be accessible by every other user in the school. Staff should not delete any files on the 'Staffroom' drive without the permission of the Innovation Lead.

Staff will ensure that they abide by copyright law. Staff will not reproduce copyright materials without first getting permission from the owner and acknowledging sources on all resources used.

All Internet activity during school hours should be appropriate to the student's education or school related work. Personal internet use is acceptable out of school hours although staff should not attempt to visit sites that may be considered inappropriate. All sites visited leave evidence on the computer. The school runs a strict filtering system but if a member of staff accesses a site on the internet which is felt to be inappropriate they will inform the Headteacher.

Use of the school network or equipment for personal financial gain, gambling, political purposes or advertising is forbidden; as is use of the network or equipment to access inappropriate materials such as pornographic, racist or offensive material.

ICT equipment should be used sensibly and appropriately. The Innovation Lead should be immediately notified if anything is not working properly or if there has been an accident of any kind.

Any use of social networking sites, e-mail, instant messaging, blogs or personal websites to engage personal attacks on other members of staff, pupils and parents is forbidden and will lead to disciplinary action.

Staff should carefully consider their interaction and use of personal social networking sites, email and instant messaging out of school time. It is not permissible to interact with or add students as 'friends', and this will lead to disciplinary action. Staff should be aware of how online acquaintances with parents and past students may look to outsiders, and this practice is strongly discouraged. Ensure privacy settings are set appropriately, particularly for photographs and social comments.

Staff will not follow or interact with students on class X (Previously Twitter) pages.

Staff should only install hardware and software that has been approved by the Innovation Lead.

Teachers are permitted to take their designated laptop and iPad home for school based work. All aspects of this policy apply out of school. Problems related to laptop use at home should be reported to the Innovation Lead at the earliest opportunity (viruses, accidental damage, unauthorised website use etc.)

Supervising children

Students will only be allowed to access the ICT facilities, including accessing the internet, when a signed consent form has been returned. The school will keep a record of returned consent forms which will regularly referred to by teachers and monitored by the Headteacher.

Students should be aware that they must only access those services they have been given permission to use. They must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.

Classroom Monitoring Software

Apple Classroom - Classroom is an app for iPad that helps teachers share work and manage student devices. It supports both shared and one-to-one environments. Teachers can launch a specific app, website, or textbook page on any iPad in the class, share documents between teacher and students, or share student work on a TV, monitor, or projector using Apple TV. Teachers can see which apps students are working in, mute student devices, assign a specific shared iPad for each student, and reset a student's password. Teachers can also access a summary of students' activities. Apple classroom has been stored on all teacher iPads. Students have individual username and passwords. Children will be unable to access iPads without a unique username and password.

Securly – Securly allows teachers to monitor and control students' laptops and PCs. Teachers can launch a specific website on students' laptops and see a thumbnail view of all screens in the class so teachers can know that their students are engaged in classwork. Teachers can check the browsing history of their students that occurred during class, while administrators can view all the history of all students.

E-Safety is continually promoted and is integral to teaching and learning practice in the school. Students will abide by the Think Then Click rules.

Students are not permitted to bring mobile phones or electronic devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the School Office to look after during the school day and collected at 3.20pm. USB memory sticks are not allowed to be used by children, but can be used to hand in homework. Teachers should extract homework from the devices and look after the device until the end of the day.

Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Staff will ensure that children's use of ICT is monitored at all times and any concerns are reported to the Innovation Lead. No child should use school ICT equipment unsupervised.

School website and social media accounts

The use of the names or photographs of students on websites will require written permission from parent(s)/guardian(s) included on the consent form. If a picture is placed on the website the child's full name will not be displayed. It should not be possible to identify a child by name from an image.

Staff are responsible for the content of their class social media pages and should ensure that it is entirely appropriate for the image of the school.

All members of staff should contact the Innovation Lead immediately if they are unhappy with any images of themselves on the website. Images will be removed or altered to the satisfaction of the member of staff.

Images of children

Staff can use their personal mobile phones and class iPad to photograph children. Staff should ensure that all photographs are removed from personal devices as soon as possible and stored on the school's shared staffroom drive. Staff understand the safeguarding implications of taking photographs of children on their

personal mobile phone and know that any allegations will be investigated in line with the Code of Conduct and with support from the Local Authority Designated Officer.

All parents are asked to give permission for images to be used within school, on the website or external publications. Staff should ensure they are aware of children who are not permitted to have their images used, and ensure sensitively that they are not used.

No images of children will be taken when a child is not fully clothed; for example in their swimming costumes.

Parents and Guardians are permitted to take images and video footage at school events. They must agree to use these images for their own personal use and not share images of other children on the internet. Anyone found breaching this agreement will not be allowed to take images or video footage at school events going forward.

Cyber Bullying (link with Anti-Bullying Policy)

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities.

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided. Children are taught how to recognise cyber bullying and of their responsibilities to use ICT safely. Think Then Click posters are displayed throughout school and are constantly referred to.

Parents are also encouraged to recognise cyber bullying and their responsibilities for supporting safe ICT use. The school provides regular parental updates on e-safety.

As with other forms of bullying, the Headteacher keeps records of cyber bullying. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

Software can not be copied illegally. Nor can illegally copied software be used on the school network. Schools can be audited at anytime. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

"Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the

Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Appendix

i) KS1 Think then Click Poster

ii) KS2 Think then Click Poster

iii) E-Safety Incident Log

Think then Click

WINTHORPE PRIMARY SCHOOL
learning together - growing together

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.

We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

WINTHORPE
PRIMARY SCHOOL
learning together - growing together

These rules help us to stay
safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	