E- SAFETY POLICY

Reviewed: June 2026

Next Review: June 2027

Our e-safety policy will operate in conjunction with other policies including those for pupil behaviour, anti-bullying, curriculum, data protection and security.

It involves all members of staff from the Headteacher to any new member of staff. Through its compliance it will ensure that everyone knows and understands their responsibilities and can act upon them.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school has appointed an e-Safety coordinator – Matthew Wiley.
Our e-Safety policy has been written by the school and been agreed by the senior management team and approved by the governors.

The e-Safety Policy will be reviewed annually.

Why is Internet Use Important?
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 information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Improve Learning?
Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, 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 with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Code of Conduct' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to Edulincs helpdesk via the e-safety coordinator.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- Our school will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering
The school will work in partnership with Education lincs to ensure that appropriate filtering and monitoring systems are in place. The senior leadership team and e-safety coordinator will receive regular reports and alerts regarding inappropriate content and take immediate action to address any concerns.

Managing Emerging Technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile Phones
Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Web Site
The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Parents will give explicit permission to use their child's image on the school website as part of their enrolment.
- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- We will, from time to time, publish pupils' work.
- If you decide at a future date that you do not wish for your children's image to be used on the school website, or any other content, then please contact the head teacher to remove the image.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and Edulincs.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Lincolnshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy
Pupils
Rules for Internet access will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored.

Staff
All staff will be given the School e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
Parents
Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

School Rules for the use of the Internet and Email - signed by all pupils and parents

When using the computers, I will: -

1. Always behave sensibly, respecting other members of the school.
2. Only log in using my own name.
3. Keep my password secret if I have one.
4. Never purposely access any material on the network, which may be considered offensive by others.
5. Close down any offensive material, which has been accessed by mistake, and report it to my teacher.
6. Be polite at all times, both to those around me and those that I contact through the network.
7. Report any offensive messages I receive through the network to my teacher or head teacher.
8. Not waste my time playing non-educational games.
9. Not download any games or other programmes without the permission of my teacher.
10. Never enter my address, telephone number, photograph or any other details about me or anyone else.
11. Only enter the school address after I have got permission from my teacher, and will never enter the school telephone number.

If any of these rules are broken, I will report it to my teacher as soon as possible.

Social Networking - social networking sites (for example TikTok, Facebook, Snapchat) are not allowed in school.
If you use them at home, you should: -

- Never upload pictures or videos of others without their permission.
- It is not advisable to upload pictures or videos of yourself, videos and pictures can easily be manipulated and used against you.
- You should never make negative remarks about the school or anyone within the school.

- Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc.
- Consider using a nickname and only inviting people you know. Universities and future employers have been known to search social networking sites.
- Beware of fake profiles and people pretending to be somebody else.
- If something doesn't feel right, follow your instincts and report it to an appropriate adult.
- Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.
- Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise.
- It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Security - you should never try to bypass any of the security in place on a school site, this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Useful websites:
CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website. www.ceop.gov.uk IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. www.iwf.org.uk BBC - a fantastic resource of e-safety information for the younger child. www.bbc.co.uk/cbbc/help/web/staysafe Cybermentors is all about young people helping and supporting people online. www.cybermentors.org.uk Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same. www.digizen.org

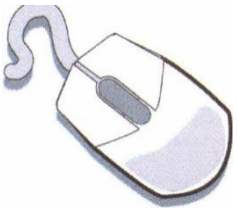
Digby the Tedder Primary School

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

Think then Click



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.

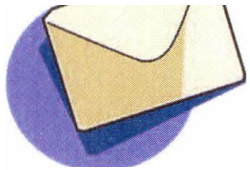


We never arrange to meet anyone we don't know.

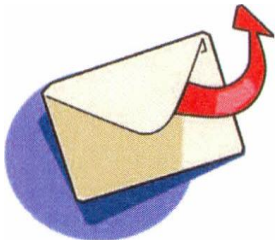
We never open e-mails sent by anyone we don't know.

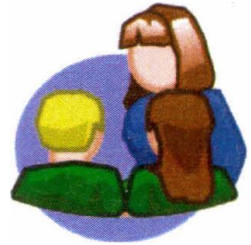
We never use Internet chat rooms.











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

STAFF CODE OF CONDUCT FOR ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

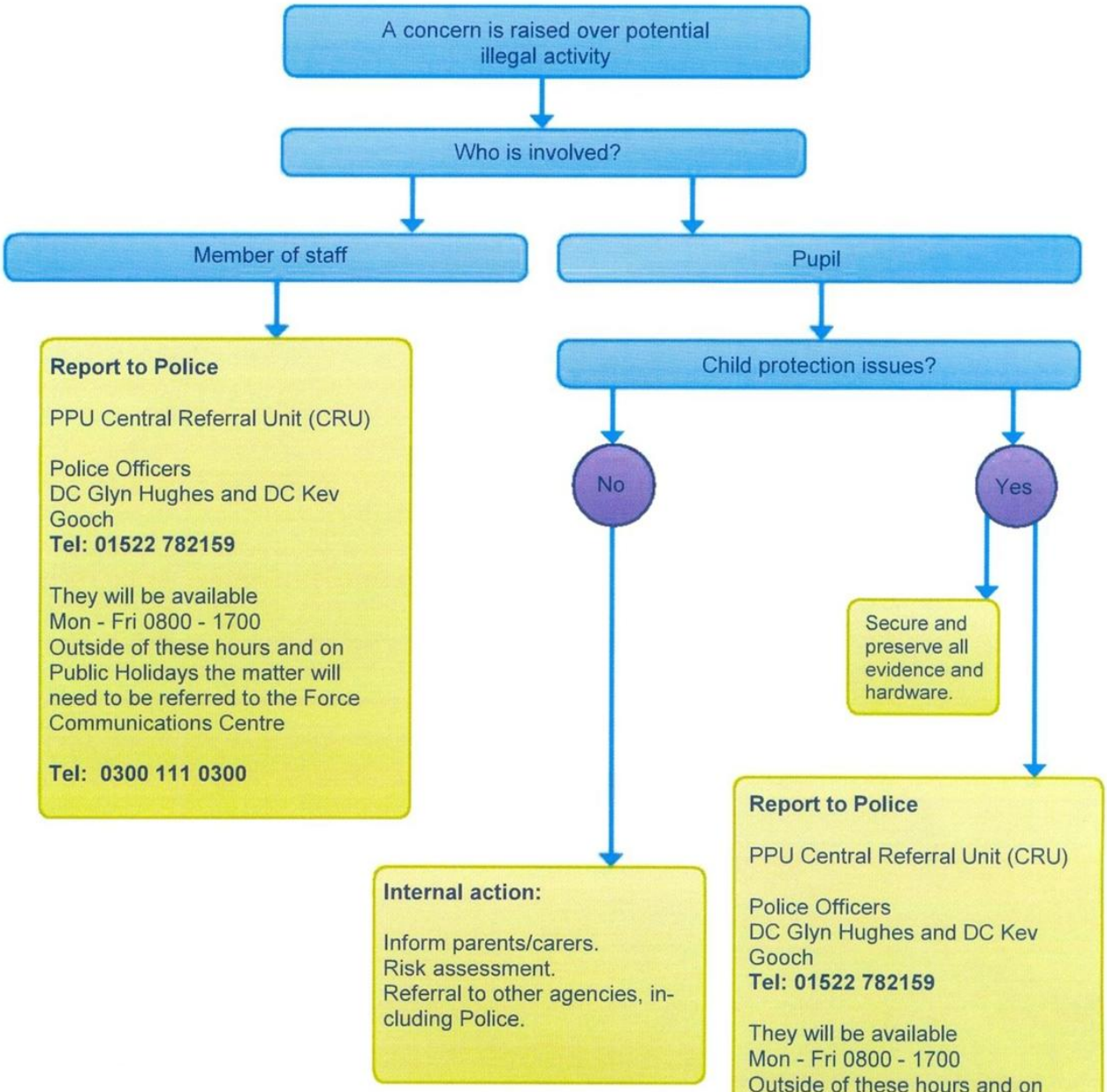
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: ……
Name: …… Date:…….
Accepted for school: ……
Name: ……

Illegal Activity flowchart



Under no circumstances should any member of staff investigate if illegal activity is suspected. By doing so you may compromise and/or commit further offences.

For example, a member of staff emails to you a picture which has been found on another person's computer. The picture looks to be a young person in a state of undress or sexually provocative. You email this to the Headteacher to ask for advice.

Within these 2 emails, two offences of distributing images of child abuse have been committed.

Inappropriate Activity flowchart

