

# Nayland Community Primary School

## Policy for E-Safety and the Acceptable Use of ICT

Autumn 2023

---

### Use of computers in general

- The use of school computers by pupils is permitted for purposes as directed by the school.
- The school has the right to look at any files on their systems including text, graphics and e-mails.
- Users are not permitted to access and or amend another's work without permission.
- Users must not give access passwords to other users.

### Remote Learning

Nayland School ensures that all pupils have access to RM Unify launch pad to ensure a safer route to frequently used sites and apps as well as OneNote and Teams to support remote learning.

### Precautions taken against computer viruses:

- All computers connected to the Internet are virus protected by AVG anti-virus software, which is up-dated regularly. Any infections are to be reported to the ICT co-ordinator/technician who will then remove the source if known.

### Sanctions for the misuse of computers:

- The school reserves the right to deny access to school computer systems, including the use of the Internet and e-mail. This may have a negative impact on a pupil's education.

### Internet Access

- The school provides Internet access for educational purposes and should only be used by pupils, staff and other members of the community for these purposes.
- Pupils follow the age appropriate **e-safety rules/acceptable use agreement** displayed in all networked rooms and shown in Appendix A.

### Steps taken to prevent access to illegal, defamatory and potentially offensive material:

- The school uses the Suffolk County Council recommended Internet Service Provider and connects to the Internet via the filtered service. Pupils cannot use computers without filtered access (The use of the filtered system cannot guarantee that pupils will not encounter material that may be deemed unsuitable).
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

- Where reasonably possible, all Internet access by pupils is supervised by a member of staff or other responsible adult.
- No pupil, member of staff or community user is permitted to access or distribute material that is illegal, defamatory or potentially offensive using school systems.
- The copyright and intellectual property rights of material accessed using school systems must be respected.
- Parents are made aware of the use of the internet for school learning through school publications and the school's website.
- The school has a legal responsibility to report the discovery of materials that are thought to be offensive or confidential to the police if necessary.

### **The use of E-mail**

- Pupils will be given e-mail access at the discretion of staff. Class or group e-mail addresses will be used for most purposes.
- Any user of the school e-mail system must not use the system to communicate offensive, suggestive or defamatory material. It must not be used to harass another individual.
- E-mail messages sent and received from school systems should not be considered private. Pupils and staff should expect that e-mails could be inspected at any time.

### **Social Networking**

- Chatrooms, blogs and other social networking sites are blocked by school filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils and the appropriate use of Nayland Primary School app for the older children.
- Pupils will be advised on the dangers of revealing personal details of any kind that may identify themselves or other pupils.
- Parents and pupils are advised that the unsupervised use of social network spaces outside school is inappropriate for primary aged children.
- Pupils are encouraged to interact with only known friends and family over the internet and deny access to others.
- Parents, pupils and staff are advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors may consider taking legal action, where appropriate, to protect pupils and staff against cyber-bullying and defamatory comments.

### **Use of Mobile phones**

- Pupils are not permitted to use mobile phones in school at any time
- Staff members are asked to leave mobile and wearable devices in a secure location, they will only be carried during class times in exceptional circumstances at the discretion of senior leaders (e.g. family medical emergency).
- The recording, taking and sharing of images, video and audio on any personal mobile or wearable device is to be avoided, except where it has been explicitly agreed by the headteacher. All mobile device use is to be open to monitoring and scrutiny and the headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.

### **Publishing on the Internet**

Responsibility for content of the school web site rests with the Head Teacher.

These guidelines will be followed:

- The school is appropriately registered under the Data Protection Act.
- Individual pupils will not be identifiable by name.
- Names will not be linked to pictures or individual e-mail addresses.
- No personal information will be published without the individual's permission – this includes staff and other community users.
- Parental consent will be sought prior to any reference – text, audio or picture - to a child or children being published.
- Systems have been put into place to ensure, where appropriate, information published is kept up to date.
- No copyright material will be published without the copyright owner's permission.
- Links will not be made to web sites which contain material deemed to be unsuitable.
- Access to web space will be restricted to ensure that only those with appropriate authority can publish to the school web site.

### **Electronic Storage of Data**

- All data, in particular personal data, should be stored on a password protected device and stored on the school's agreed cloud storage.
- No personal data should be stored on mobile devices, whether such device belongs to school.
- Data may only be stored on the school's computer network for it to be backed up.

Agreed by Governing Body: TBC

Annual Review: Autumn 2024

## E-safety Rules for Key Stage 1

Think before you 'Click'

These rules help us to stay safe on the internet...

- 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 Rules for Key Stage 2

Think before you 'Click'

These rules help us to stay safe on the internet...

- We ask permission before using the internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything with which we are uncomfortable.
- We immediately close any web page we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use internet chat rooms.

**Nayland School**  
**Y5/6 Pupil Acceptable Use Agreement 2021**

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
3. I will only edit or delete my own files and not view, or change, other people's files without their permission.
4. I will use the Internet responsibly and will not try to visit web sites I know to be inappropriate to school. I am also aware that during lessons I should only visit web sites that are appropriate for my studies.
5. I will only e-mail people I know, or those approved by my teachers.
6. The messages I send, or information I upload, will always be polite and sensible.
7. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
8. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
9. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
10. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.
11. I am aware that some games, websites and social networks have age restrictions and I will respect this.

12. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.  
*I have read and understand these rules and agree to them.*

*Signed:*

*Date:*

*Always alert the SDL (R. Delaney) or alternate (K. Coburn) safeguarding if you feel the behaviour of any child may be a cause for concern.*

*It is your duty to support a whole-school safeguarding approach and report any behaviour of other staff or pupils, which you believe may be inappropriate or concerning in any way, to the headteacher or deputy headteacher.*

*As a member of the Nayland School staff, you have a responsibility for your own and others e-safeguarding and must undertake to be a 'safe and responsible digital technologies user' both in and out of school.*

*It is your responsibility to ensure that you remain up-to-date and read and understand the school's most recent e-safety policies.*

---