Marazion School
Online Safety Policy to include Cyberbullying and Guidelines on Mobile Phone Usage

Reviewed November 2021 by Headteacher; iCT4 Technician; Staff/Governor Lead on Online Safety

Approved November 2021 by FGB

ICT Online Policy
Appropriate use of internet and email facilities

1. Rationale

The Internet is becoming as commonplace as the telephone or TV. Significant educational benefits should result from curriculum internet use, including access to information from around the World and the ability to communicate widely.
Internet safety depends on staff, schools, governors, advisers, parents and carers to take responsibility for the use of the Internet.

- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. The purpose of internet use in school is to:
    - raise educational standards
    - promote pupil achievement
    - support the professional work of staff
    - provide an audience for pupils' work
    - develop pupils' skills and knowledge in order to use technology
- One of the benefits of using the internet is access to world-wide educational resources including museums and art galleries. Staff will adapt an ethos to promote safe use to ensure that users only access appropriate material.
- Pupils have regular reminders about rules, guidelines and useful information for internet access as well as annual online safety training
- Virus protection is installed and updated regularly across the entire school.

- The ICT and internet facilities are available to all Marazion School children, staff and Governors.
- There are opportunities for parents of children in the school to access the internet via schools facilities as arranged with a member of staff. This allows parents to feel confident enough with ICT to support their children's learning at home. This facility is available at parents' request.

2. Responsibilities for Online Safety

Staff Lead for Online Safety: Lewis Groom and Laura Holmes
Link Governor for Online Safety: Jim Allen

3. Principles for Acceptable Use of the Internet

Use of school computers by pupils must be in support of the aims and objectives of the Primary National Curriculum.

4. Safeguarding training

Safeguarding training for staff, including online safety training, and the requirement to ensure children are taught about safeguarding, including online safety, must be integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning. Reference should also be made to the Teachers' Standards – the expectation that all teachers manage behaviour effectively to ensure a good and safe educational environment and that teachers must have a clear understanding of the needs of all pupils.

Online activities which are encouraged include:

- Use of the internet to investigate and research school subjects, cross-curricular themes or topics.
- The development of pupils' competence in ICT skills and their general research skills
- Use of the internet to support homework and further study
- Use of Seesaw as part of Marazion School's Remote (Home) Learning Offer

Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum.
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering any goods or services, unless specifically approved by the school.
- Playing computer games or using other interactive 'chat' sites ***unless specifically approved by the school.***

- Using the network in such a way that disrupts/hinders other users (for example: downloading large files during peak usage times; streaming live sports/news feeds).
- Publishing, sharing or distributing any personal information about a user (such as: home address, email address, phone number etc).
- Downloading software without permission from the Schools Network Manager.
- Downloading software/scripts without permission from the School's Network Manager
- Any activity that violates a school rule
- Any use of scripts is not permitted without approval from head teacher/iCT4.

5. Guidelines (for specific guidance, please see Appendix A).

Children will:

- Have equal access to a variety of approved websites through the Intranet.
- Be taught all the skills in order to use internet & email as an ICT tool.
- Use internet & computing to support, enhance & develop all aspects of curriculum.
- Develop internet & computing skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.

Appendix A

Guidance on the use of email

Certain pupils perceive email as a way to send secret offensive messages. Anyone receiving unwanted email should report it immediately to the school's IT Subject Leader or any teacher. Anyone caught sending such messages will have their access to the technology restricted. Please note that staff must make take care when forwarding email content or adding email recipients to an existing email. Staff must make sure that all of the information on the email is suitable for all recipients, in particular when forwarding long email threads.

General Guidance for All Users

- Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees in the Information Age. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use, and provide guidance and instruction to pupils in the acceptable use of the Intranet/Internet.
- It is not permitted for staff to invite or accept pupils onto personal social networking sites – refer to Marazion School's General Code of Conduct.

- Staff should be very sensitive to the content of any material they post on social networking sites given the audience. Some comments could be perceived as inappropriate or unprofessional. Such comments could lead to disciplinary action. Please remember you are a professional – please refer to *Marazion General Code of Conduct* / *Teachers Standards* document
- Staff should be aware of Cornwall Council's *Social Networking Guidelines.*
- Cornwall LA supports the implementation and sharing of effective practices and collaborative networking across the LA as well as nationally and internationally. Please select appropriate websites to collaborate and ensure you are aware of the audiences.
- When using the internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behavior governing employees in the education sector.
- Pupils are responsible for their good behaviour on the school networks, just as they are on and off school premises. While the use of information and communication technologies is a required aspect of the National Curriculum, access to the Intranet/Internet is a privilege – not a right. It will be given to pupils who act in a considerate and responsible manner, and may be withdrawn if they fail to maintain acceptable standards of use.
- Staff should ensure that pupils know and understand that, in addition to the points found under **Online activities which are not permitted** on page 2 of this document, no Intranet or Internet user is permitted to:

    - Retrieve, send, copy or display offensive messages or pictures.
    - Use obscene or racist language.
    - Harass, insult or attack others.
    - Damage computers, computer peripherals, computer systems or computer networks.
    - Violate copyright laws.
    - Use another user's login account.
    - Trespass in another user's folders, work or files.
    - Use the network for commercial purposes.
    - Use the network to promote extremism of any kind

Supervising and Monitoring Usage

Teachers should guide pupils toward appropriate materials on the intranet/internet. This will avoid a great deal of time wasting as well as going some way towards monitoring the sites accessed by pupils.

Internet access for pupils in schools should be available only on computers that are in highly-used areas of the school such as classrooms, library, study rooms, computer

rooms and the media room. Machines, which are connected to the intranet/internet, should be in full view of people circulating in the area. Children should never use intranet/internet services without supervision.

While using the internet at school, pupils should be supervised. However, when appropriate to their age and their focus of study, pupils may pursue electronic research independent of staff supervision; this should be at the discretion of the teacher in charge. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the internet itself, users must not expect files stored on school servers to be absolutely private. An email is as private as a postcard, it is quite likely that no one other than the sender and receiver will ever read it, but others could if they were inclined.

Filtering External Websites

It is an absolute requirement that access to the Internet provided to staff and pupils in any school or educational institution through any Internet Service Provider (ISP) is a filtered service. *iCT4* offers a managed filtering service, and is updated regularly. The School Network Manager has access to improve this filtering whereby if a user discovers an unsuitable website, this can be immediately filtered. All users should be aware that the *iCT4* keeps a log of internet traffic, tracking and recording sites visited and the searches made on the intranet/internet by individual users. iCT4 use *Sonicwall* as the filter and *Senso* software, which sends instant email alerts to the Business Manager (Edna Smith) so a potential concern an be dealt with quickly and appropriately.

Schools should advise parents that they provide filtered and monitored access to the internet for pupils. However, they should also be aware that with these emerging and constantly changing technologies there is no absolute guarantee that a pupil cannot access materials that would be considered unsuitable. The chance of just coming across such materials is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort individuals put into their search. If you are unfortunate enough to come across any offensive web pages, whilst using school equipment, you are obliged to make a note of the address and report it to the ICT Subject Leader, External ICT Support Provider or the Headteacher, who will then pass it on to the iCT4. The ICT technician will then take the appropriate action to block the site.

Our initial aim is to provide intranet/internet access to all teachers, in order to enhance their professional development. It is however understandable and desirable that the equipment is also being used by pupils.

Appendix B: Mobile Phones:

The school understands that some pupils are issued with mobile phones for good reason. However, if a pupil is found to be using a mobile phone, it can be confiscated as a disciplinary penalty and school staff have a legal defense in respect of this in the

Education and Inspections Act 2006 (S94). In order to protect all staff and pupils the following rules apply:

- Pupils with mobile phones should hand them in at the office first thing in the morning and collect them at the end of the school day.
- Staff should not usually use personal mobile phones to contact parents. This safeguards their number.
- Staff mobile phones should be kept on silent during the school day.
- Should a staff mobile phone go missing in school this should be reported to the Headteacher and the Police.
- Staff should never loan their personal mobile phones to pupils.
- Any photos of pupils taken on a mobile phone should be deleted within 48 hours.
- If an outside mobile device is taken into school and is connected to the school wi-fi, then by default it will have the most restricted level of filtering. If this device belongs to a visitor / staff member, *iCT4* can able to provide "staff level" filtering access.

Related Documents: www.digizen.org/cyberbullying