Hempland Primary School

E-safety and Online Guidance

Published date:	September 2023
Review date:	September 2024
Member of staff responsible:	Gareth Dyer

Contents

Rationale

Online safety encompasses many aspects of computing and technology use in school, including (but not limited to) use of computers, tablets, mobile phones and other wireless technology. This policy highlights the need to educate children and young people about the benefits and risks of using new technology, and provides rules, safeguards, guidance and awareness for all users in school, both children and adults, to be able to control their online experiences.

This policy will operate in conjunction with other policies, including (but not limited to) Child Protection and Safeguarding policy, Behaviour policy, Home-School Communication Policy, Acceptable Use policy and the Data Protection policy.

Teaching and Learning

Internet use in schools is important:

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- The purpose of the 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 business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely inside and outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use by pupils will enhance learning:

- The school Internet access is planned expressly for pupils' use and includes monitoring of, and filtering appropriate to the age of pupils.
- Pupils are 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 guide pupils in on-line activities that supports the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Identifying risks

Content – these are risks related to content that the children could encounter online.

- ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases)
- exposure to inappropriate content, including online pornography,
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.
- data breach

- hate sites, sites inciting radicalisation and/or extremism
- content validation: how to check authenticity and accuracy of online content

Contact – these are risks that the children might encounter related to contact with other people, either known or unknown.

- Grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct – these are risks that could arise as a result of how children might behave online.

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Inappropriate Messaging

Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school takes *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.* Neither the school nor the Pathfinder MAT can accept liability for the material accessed, or any consequences of Internet access. However, any access will be assessed and reasonable safeguards put in place to prevent a recurrence.

Methods to identify, assess and minimise risks are reviewed regularly.

Managing risks

Content

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is part of every subject.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported, where appropriate, to the school business manager or Computing leader, who will take the necessary action ie: report to the Portal.

Contact

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

- Pupils are advised and educated about security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.

Conduct

- Pupils are advised not to, and educated about the risks of, signing up to any social networking site that is not age appropriate. eg. Facebook
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline telephone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They are educated to consider how public the information is and when and how to use private areas. Advice is given regarding background detail in a photograph which could identify a pupil or his/her location eg: house number, street name, school or shopping centre.
- Staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of any images.
- Pupils are taught about staying kind online in Key Stage One, and about online reputations and digital footprints in Key Stage 2.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Pupils are advised not to publish specific and detailed private thoughts.
- Pupils are informed that Internet use is monitored.
- Online access is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. Online safety education is broad and relevant with progression related to the age and development of pupils. This is influenced by the 'Education for a Connected World' framework and the Teach Computing framework.
- Instruction in responsible and safe use precedes all Internet access.
- The School ensures that the use of Internet derived materials by staff and by pupils complies with copyright law.
- The security of the school information systems will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Portable media (e.g. pen drives) should not be used in school.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.

Staff awareness and training

Teaching staff:

- have an up-to-date awareness of online safety matters, know the current policy and follow good practice
- guidelines. They are kept up-to-date with information through staff INSET, guidance information and self-study.
- Abide by the PMAT Acceptable Use policy and the staff Code of Conduct.
- Report any suspected misuse, by pupil or adult, to the Headteacher, School Business Manager or Computing lead
- as soon as possible.
- Ensure that any online communication with pupils or parents is professional (see Home-School Communication Policy)
- ensure that online safety is planned for and embedded into their teaching.
- monitor the use of digital technologies, (e.g. iPads/ Chromebooks etc) by pupils, and implement policies where applicable.

All staff:

- will receive online safety training which is updated as new information or technologies arise. Training is refreshed each year as part of the annual safeguarding review.
- respond to online safety concerns involving staff or pupils promptly.
- when new, receive online safety information as part of their induction.
- when new, receive the PMAT Acceptable Use Policy and Online Safety policies as well as the Code of Conduct as part of their induction.
- will be provided with advice, guidance or training as requested or as identified through performance management procedures.

Safe use of technology – Students

To be used with the PMAT Acceptable Use Policy

For my own personal safety:

- I understand that the school will monitor my use of the Computing systems, emails and other digital communications.
- I will treat my username and password safe and only share them with trusted adults.
- I will not disclose or share personal information about myself or others when on–line.
- I will not arrange to meet people I have met only online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a trusted adult.

I understand that everyone has equal rights to use technology as a resource, and I understand that the school Computing systems are primarily intended for educational use, and that I will not use the systems for personal or recreational use unless I have permission to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility keep me safe, and look after the technology in school:

- If I bring a mobile phones, tablet or smart watches into school, it must be turned off **upon entry onto school grounds**, (not placed on silent) and handed in to my class teacher on arrival at school/ handed into the school office to be locked away. It will be returned at the end of the day and must not be turned back on until I have left school grounds.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not use my school e-mail account unless I have been direct to by a teacher.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites on school equipment.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement. This applies both in school, and when I am out of school where it involves my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this agreement, there will be consequences for my behaviour (see Behaviour Policy). This may include loss of access to the school digital devices, contact with parents and, in the event of illegal activities, involvement of the police.

Safe use of technology - Staff

To be used alongside the PMAT Acceptable Use Policy

Any personal or business use of school technology for illegal, threatening, offensive, obscene, pornographic or libellous purposes by staff is strictly prohibited

Passwords

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for all school systems.

Email - (To be used alongside Communication Policy)

- School will provide staff with an email account for their professional use.
- Will contact the Police if one of our staff receive an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Access in school to external personal e-mail accounts, on school devices, during working hours is not permitted and may be blocked
- Never use personal email to transfer staff or pupil personal data.
- Emails should only be used during lesson times in exceptional circumstances.
- A letter sent to anyone using the school letterhead must be approved by the member of the Senior Leadership Team.

Personal mobile phones and mobile devices

For this section "mobile phones" includes all mobile smart devices, including tablets and smart watches.

- Mobile phones brought into school are entirely at the staff member, parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- All visitors and staff are requested to keep their phones on silent during lesson times.

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Staff may use their phones during break times in an appropriate location (staff room/ empty classroom etc). Corridors, or any areas where children are present, are not appropriate locations. If a staff member is expecting a personal call, they may leave their phone on and they may seek specific permissions from the head teacher to use their phone at times other than their break times.
- Staff mobile phones and personally-owned devices (including smart watches) will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. Non-Classroom based staff should not use mobile phones or smart watches during their working hours, unless previously approved by the head teacher.
- Images and content recorded for twitter updates will be deleted from the school equipment once it is posted.

Staff use of school devices (e.g. laptops and ipads) must adhere with the GDPR policy.

Use of Social Media (staff)

- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of school events on personal social networking sites such as Facebook. Twitter etc
- Staff must not use social networking sites within lesson times, or during working hours for non-Classroom based staff.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy.

Safe Use of Technology - Parents/ Visitors

- Parents/carers/visitors are not permitted to use their mobile phones/take pictures and/or videos of staff and/or pupils unless otherwise informed. No pictures or videos which include children other than their own may be shared online.
- When communicating with school, parents/ carers should email school according to the school communication policy.
- Parents/ carers should be up to date with the various risks associated with their children using online technology, particularly related to communication (e.g. social media) and content.
- Parents/ carers are responsible for their child's use of online technology when the children are outside of school.
- Parents/ carers support the school in promoting e-safety and engage with documentation shared by the school.
- School will run a rolling programme of advice, guidance and training for parents, including information in the weekly newsletters, on the school website, sessions held within school and sharing of national support sites for parents.
- If helping on school trips, parents/ carers must adhere to the same photograph rules as staff (e.g. no photographs on personal devices).

School procedures

Use of digital images

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications, the school will obtain individual parental or pupil permission for its long term use;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Photos/videos taken on school iPads are stored on the school network, and deleted from iPads as soon as possible.

Published content and the school website:

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information is not be published
- Email addresses are generally not published, to avoid spam harvesting. Contact forms are used where possible.
- The Headteacher takes overall editorial responsibility to ensure that content is accurate and appropriate.
- The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing staff and pupil's images and work:

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parents or carers are asked each year if they give permission for the school to use their child's photograph in school publications (which includes the school website).
- Images of staff are not published without consent from that member of staff.