Hunnyhill Primary School

Date of Review	**November 2020**
Next Review Due	**November 2022**
Staff Responsibility	Computing Lead / Headteacher
Notes / Source	
Signed by Chair of Governors	P Stevens

Adult E-Safety Policy

Aims

The aim of this policy is to make clear the expectations and requirements that the school has of all users of computers, IT equipment and Internet provision within the school.

The school recognises that Computing is an important part of school life and the education system and the responsibilities that come with it are taken very seriously.

Staff, Volunteers and Governors

All persons with access to computers in relation to their work in the school are expected to adhere to the following Code of Practice for safe use:

1. This code covers not only school based technologies but any personal technologies brought onto the school site.
2. When using the Internet, email systems and other digital technologies all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity.
3. Users will not install any software or application that is not for school use on school equipment. All software and applications must have a school owned valid licence and be approved by the school.
4. All staff are expected to communicate in a professional manner, both internally and externally, consistent with the Staff Code of Conduct and the Social Media Policy
5. Whilst normal privacy and confidential Items are respected and protected, users may not expect files and messages on publicly funded networks to be private. (See Confidentiality and Data Protection Policies)
6. All internet site visit histories and communications on the school system may be examined by the relevant person at any time. The relevant person is the Headteacher or a person directed by the Headteacher, usually the network administrator or the School Business Manager.
7. No part of the school system may be used for non-work or social networking other than those directly involved in education purposes such as communicating with another school.
8. No user is permitted to disable or attempt to disable the school's security system.
9. Confidential information must not be transferred to computers outside the system without the express permission of the Headteacher.
10. Users should be aware that postings on other sites outside the school system which refer to the school or its staff and which bring the school into disrepute will be subject to misconduct proceedings and/or legal proceedings. (See Disciplinary Policy and Social Media Policy)

11. Users will adhere to the rules of any other school or Local Authority property where they may be using IT equipment.
12. No user will give out their personal details, email etc. to children. Contact with children at this school on social networking sites is not allowed.
13. Any school equipment, such as a laptop or tablet, issued to any member of staff is to be used for school purposes only.
14. Adults will sign the Computing Use Agreement.

Monitoring and Review

- An inventory of ICT asset register is electronic and maintained by IWEF. The signed paper forms are kept is staff personell files.
- Acting on behalf of the school, IWEF review of firewall and blocking procedures will be on-going as technology is consistently changing.
- Any equipment loaned to staff, such as laptops or tablets, will be signed for.
- This policy will be reviewed on a yearly basis and should be read in conjunction with the highlighted policies above.
- Any incidents using computers and the internet which give rise to concern will be notified to the Headteacher and if necessary recorded in the Safeguarding log.

How will email be managed?

Email is an essential means of communication within education and the government is encouraging the ownership of personal email Ids for both teachers and children. Children need to use email as part of the National Curriculum.

The following rules for email use will be as followed:-

- Email must only be used in school for educational purposes.
- Incoming email will be regarded as public. Received email may be examined and could, for example, be pinned to a notice board.
- Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper.

How will publishing on the Web be managed?

Many schools have created Web sites that inspire children to publish work to a high standard, for a very wide audience. A Web site can celebrate children's work, promote the school and publish resources for projects or homework. Ground rules are important to ensure that the Web site reflects the school's ethos and that information is accurate and well presented.

As Hunnyhill's Website can be accessed by anyone on the Internet, the security of staff and children is paramount. Although common in newspaper reports, the publishing of children's names beside photographs that identify individuals will not occur and forenames will only be used.

Editorial responsibility will lie with the Headteacher and Computing Lead. This is in order to ensure that content is accurate and quality of presentation is monitored.

Staff and children will be made aware that the quality of their work published on the web needs to reflect the standard of work expected at Hunnyhill.

- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name

- The point of contact on the Web site should be the school address and telephone number. Home information or individual email identities will not be published.
- Full names will not be used anywhere on the Web site, particularly alongside photographs.
- Written permission from parents will be sought to give permission for the school to use photographs of their children on the website.

How will staff and children know what is expected of them?

- Rules for Safe Use of Internet access is an integral part of the school curriculum.
- All staff including teachers, supply staff, classroom assistants and support staff and parents will be made aware these rules, and their importance explained.
- Parents' attention will be drawn to the Policy on the school Web site.

How will the risks be assessed?

It is difficult to remove completely the risk that children might access unsuitable materials via the school system whatever safeguards are put in place.

- Due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.
- Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences thereof.
- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed at the same time as the policy is reviewed.
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken.
- The Curriculum Leader for Computing and the headteacher will ensure that the policy is implemented effectively.

How will the school ensure Internet access is safe?

- The system the school will use is a blocking system.
- Children will be informed that internet use will be supervised and monitored.
- The school will work in partnership with parents; the LA, DfE and the Internet Service Provider to ensure systems to protect children are reviewed and improved.
- Teachers will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice
- In the unlikely event that staff or children discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider via the Curriculum Leader for Computing and blocked through the schools computer filters.

How will the security of school computing systems be maintained?

- The security of the whole system will be reviewed with regard to threats to security from Internet access
- Personal data sent over the Internet will be encrypted or otherwise secured
- Virus protection will be installed and updated regularly

How will complaints regarding Internet use be handled?

- Prompt action will be required if a complaint is made. The facts of the case will need to be established as quickly as possible.
- Responsibility for handling incidents will be given to the Curriculum Leader for Computing and if further action is required the School Complaint's Procedure should be followed.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Adult Computing Use Agreement

1. I understand that these rules cover school technologies and any personal technologies that I may bring into school

2. I understand that mobile phones cannot be used during teaching time and must be kept switched off. They may be used in the staff room and carried onto the field for emergency use.

3. I will not take any images of children on personal technologies

4. I will comply with any current legislation with regard to copyright, property theft, libel, fraud, discrimination and obscenity

5. I will not install any software or application that is not for school use and only use software and applications approved by the school's network administrator and that has a valid school licence

6. I will communicate only in a professional manner, both internally and externally.

7. I understand that my school communications, internet history and any device loaned to me by the school (such as a laptop) may be examined at any time by a person appointed by the Headteacher.

8. I will not use any part of the school system for non-work items or for social networking unless it is directly connected with an educational purpose (such as communicating with another school) and approved by my line manager or the Headteacher.

9. I will not attempt to disable or interfere in any way with the school computer security system

10. I will not communicate confidential items outside the system without the express permission of the Headteacher

11. I will only use school provided and encrypted portable storage devices and not use them on anything other than school Computing equipment.

12. I will not download school information onto any personal storage device

13. I understand that it is permitted to connect a personal device to the school internet system as long as I have due regard to the rules set out here

14. I will not give out my personal details (such as email address) to children

15. I understand that communicating on social networking sites with children at this school is not allowed and will report any such contact to the Headteacher

16. I understand that any device loaned to me by the school (such as a laptop) is to be used for school purposes only

17. I undertake to take reasonable care, to the best of my ability, of all school Computing equipment

18. I am aware that any comments posted by me on any public/social network sites that could bring the school into disrepute may be the subject of disciplinary procedures for misconduct and/or legal action

19. I will ask for and observe the rules in any other school or LA workplace regarding IT

Signed..... Name..... (Print)

Personal Use of Social Media

3.1. Many practitioners will have personal social media accounts which is perfectly acceptable. Social media is a factor in modern day life.

3.2. Practitioners should ensure that their online presence is professionally appropriate and does not compromise their professionalism or reputation by those that get to see what they post.

3.3. Practitioners should remember that any post on a social media account leaves a digital footprint, even if it is later deleted. To this extent they should think carefully about anything they post, remembering they are a member of the Isle of Wight children's workforce and anything they post on social media has the potential to end up in the public arena.

3.4. Practitioners should ensure they have the correct 'privacy' or 'security' settings on their social media accounts to prevent them being viewed by individuals they may not wish to have access to their personal information.

3.5. It is worth noting that having set these privacy settings they should be checked regularly as updates, upgrades or changes in the way they are accessed could reset the privacy settings.

3.6. No practitioner should ever break the law on social media for example post racist comments or use it to share illegal images.

3.7. Practitioners should never be 'friends' or 'linked' on social media with children and young people, that use their service, including for example pupils in a school where an individual works.

3.8. Practitioners should not be 'friends' or linked to the parents and families of these children and young people unless they are related to them or they were friends before they began work at Hunnyhill.

3.9. The only exception to this would be if these people are family members or personal relationships pre-date the professional relationship. In which case the line manager should be informed and this should be recorded on an individual's supervision file with clear actions/outcomes.

3.10. An individual who is both a user of a service and a practitioner (i.e. a member of staff who's child attends the school they work in) should still use social media as if they are a professional.

3.11. Social media should not be used for practitioners to discuss work based issues, either organisational or related to individuals, as this would put these into the public arena.

3.12. If a post on social media is "liked" this could be seen as agreement with all the content related that post to date so practitioners should be mindful ,of for example, liking something that looks innocuous but earlier within it contains inflammatory or insulting remarks.

3.13. Personal use of social media should not be undertaken on any kind of equipment/devices provided by the practitioner's agency or organisation for work based activities.

3.14. Likewise if personal computers and devices are used to access social media, individuals are responsible for ensuring that these devices are not accessed by someone else afterwards who is then able to retrieve the information. If there is any uncertainty it is important to seek professional IT advice.

3.15. Personal use of social media should only be undertaken on personally owned equipment/devices. Using public devices such as in internet cafes runs the risk of others accessing personal details from this machine afterwards.

Professional Use of Social Media.

4.1. Practitioners can use social media as a positive platform for sharing ideas, knowledge and promoting their profession. In doing so they are acting as ambassadors for their profession and the children's workforce of the Isle of Wight as a whole.

4.2. Personal information of children and young people that practitioners work with should never be shared on social media/public platforms.

4.3. Likewise privileged or confidential information about colleagues should never be shared on social media/public platforms.

4.4. It is important that the children we work with learn to use social media/public platforms safely and it is everyone's responsibility to try and keep young people safe whilst they are on-line. Young people should be supported to use social media safely with awareness of its potential and risks.

4.5. Practitioners may make use of social media/public platforms for continuing professional development for example by accessing learning materials. It is important that practitioners keep their practice up to date but also be aware that such material may not be factually correct, so should validate and access its source before assuming its credibility.

4.6. If professionals have social media accounts for work that are open source material (can be accessed by anyone) they should differentiate these from their personal accounts where they may connect to friends and family members.

Organisational Use of Social Media.

5.1. Many organisations, including individuals who have businesses, use social media/public platforms to promote their business or events they are running or as a means of communication with the users of their service. This is perfectly acceptable; however it would not be acceptable to publish personally identifying information, be that about staff, volunteers or users of the service and their families.

5.2. Photographs of children should not be published without the expressed written consent of the person who holds parental responsibility. If photographs are published individual children should not be identified.

5.3. No form of bullying or abuse will be tolerated on any social media accounts.

5.4. Some social media/public accounts allow people to write comments about the information that is posted. Organisations should reserve the right to and take steps to delete comments that are abusive or insulting or break the terms of the policy. Individuals who persist in doing this should be banned from the organisations social media account and in extreme cases consideration should be given to reporting them to the relevant social media platform.

5.5. Any practitioner who persists in this posting comments that are abusive or insulting should be reported to the HR department as they may have breached the organisations code of conduct.

5.6. Practitioners should be aware that if they use their personal accounts to link to an organisational page (i.e. a teacher links their personal Facebook account to the school's Facebook account) this may allow other users of the organisational page to view their personal information.

5.7. Organisations should have in place policies and procedures to protect and support staff from harassment, abuse or hate mail as a result of their work.

5.8. Some agencies may have their own pages on social media to promote their work and services and to communicate messages to the users of their service. This would be a professional page with content of an organisational nature and as such should not be used by individuals to communicate personally with users of the service. If members of the children's workforce link to these sites they run the risk of other users being able to see their own content

Use of Social Media as an Assessment Tool

6.1. Social media accounts are a good way of having a better understanding of an individual's life and there may be justification for accessing someone's personal social media accounts if they are open source material.

6.2. Social media accounts give an opportunity to see beyond what and how individuals present to professionals during assessment visits.

6.3. It could be considered proportionate to view an individual's social media account to seek evidence to confirm or refute something that may be a concern (child safeguarding). This decision should be made on a case by case basis with a recorded view why this is being done, by whom and should always consider who is best placed to do it. If done from a personal account you run the risk of leaving a digital footprint for that individual to know you have accessed their information, therefore this should only be done from an organisational device/account and before doing this individuals should seek line manager approval for doing this and the rationale should be clearly recorded. This should only be done for concerns of a child protection nature and not 'to be nosey'.

6.4. Organisations who wish to do this should consider including a reference to it in their information sharing policy that… "In order to protect your child(ren) and provide the best possible service, we may sometimes need to gather information from other agencies and sources both on and off-line."

6.5. If an organisation or its workforce do view a service user's social media account and there is relevant information to a child protection concern on there, they may consider taking a screenshot of this. Screenshots have previously been admissible in court as evidence. That a screenshot has been taken should be recorded in the service user record, by whom and for what purpose, along with information gleaned and a copy of the screenshot.

6.6. No individual's social media account should ever be 'hacked'.

6.7. Practitioners should never link their personal accounts to other individuals they are working with, with a view to taking a look at that individual's personal information and posts, because this in turn could allow other people to see their own information.