Farlingaye HIGH SCHOOL

Online Safety Policy

Equality Statement

Farlingaye High School values diversity, and is determined to ensure that everyone is treated fairly, with dignity and respect; where the opportunities we provide are open to all; and that we provide a safe, supportive and welcoming environment - for staff, students and visitors.

Equality Impact Assessment (EIA)

This policy has been assessed with regard to its impact on equalities issue, with specific reference to the aims of the Equality Act 2010. The equality impact assessment focused on race, gender, disability, pregnancy and maternity, age, sexual orientation, gender identity and religion/belief.

EIA outcomes

• No areas of potential negative impact were found and actions resulting in positive impact are in place where appropriate.

Date Drafted (D) or Reviewed (R)	Agreed by Governors	Review Date (For review every 2 years)	Statutory Requirement (SR) Best Practice (BP)	Person Responsible	On website
April 2019	TBA Dec 2019	Dec 2021	BP	AS/JM	
September 2021	September 2021	September 2023	SR	AS/CH	Yes

Farlingaye High School Online Safety Policy

Updated by: Miss C Hankers (Safeguarding Manager/ Alternate Designated Safeguarding Lead / Online Safety Lead)
Date: September 2021
To be reviewed: every other year

Introduction and Educational Purpose:

The FHS Network/Internet access has been established for an educational purpose. The term "educational purpose" includes classroom activities, career development, and quality research activities. Children and young people will need to develop ICT skills to support their learning in school and also to prepare themselves for future learning and employment. The benefits of using ICT in school are seen to outweigh the risks. However, schools must ensure that their Online Safety Policy meets statutory obligations to ensure that young people are safe and protected from harm both with their personal online safety usage outside of school and their online safety usage in school as part of their education. As a school we will take a contextualised safeguarding approach and will risk assess and take appropriate action on a case by case basis.

Risks associated with online use:

The breadth of issues classified within online safety is considerable, but can be categorised into 4 areas of risk, according to 'Keeping children safe in education 2021':

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **Contact:** Being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams

This is not an exhaustive list of risks. Many of these risks and issues could also be in conjunction with offline issues. Therefore, this policy must also be used in conjunction with other school policies (eg: Behaviour Policy; Bullying Policy; Data Protection GDPR Policy; Peer-on-Peer Abuse Policy; PREVENT duty and our Safeguarding Policy).

The Senior Leadership Team, Safeguarding Team or Year Teams will follow our Safeguarding Policy or Peer on Peer abuse if it is felt that a pupil is at risk of harm either through their own online behaviour or the online behaviour of someone else. Staff in these teams may pass information on to CEOP (Chid Exploitation and Onine Protection Services) the Police or Children and Young People's Services (CYPS) if it is considered a multi-disciplinary approach is needed to keep a pupil/pupils safe.

Online Safety issues which may be reported to the Police or Children and Young People's Services by Staff or Parents/Carers include, but is not limited to:

- Malicious messaging including abusive or threatening text messages.
- Pupils under the age of 18 sharing nudes or semi-nude imagery. Under the Sexual Offences Act 2003 Taking, making, sharing, distributing and possessing indecent images and pseudo-photographs of people under 18 is illegal regardless if they have consented to their image being shared.

- Cyber Crime including hacking, making, supplying or obtaining malicious software such as viruses.
- If we have evidence to belive a pupil is at risk of Child Sexual Exploitation (CSE), Child Crimal Exploitation (CCE) or radicalisation.
- If a pupil is sending, promoting or distributing hate crime material.

Parents/Carers also have the responsibility to report any of the above to the Police if they believe their child is at risk. In the event that information needs to be reported to the Police,staff and Parents/Carers will report the above online safety issues to Suffolk Constabulary by either ringing 101 or reporting information via their website: https://www.suffolk.police.uk/contact-us/report-something Farlingaye have a duty to report the behaviour listed about to the Police or CYPS, regardless if it did not happen on school site or using a school computer or a school email address.

As per our Building relationships policy Farlingaye takes a zero tolerance approach to bullying whether this be face to face or online, however we are aware that young people do abuse their peers regardless of age or gender. The Behaviour Policy will be followed if staff have been given information to suggest a pupil is using the school online systems to cause distress or upset to another student. Staff will investigate the following use of school computers or emails:

- Sending abusive or threatening texts, emails or messages.
- Sharing humiliating or embarrassing videos of someone else,
- Stealing someone's identity.

Use of Internet Facilities:

1. Before accessing the school network, all pupils and their parents/guardians must sign an 'Online Safety Rules' document (Appendix A)
2. All pupil Internet access must be supervised (*with the exception of 6th form pupils*). This means there **must** be a member of staff in the room who is aware that the pupil is accessing the Internet. If the member of staff leaves the room then pupils must stop using the Internet.
3. Inappropriate Access to online material -
    a. Internet access is filtered through our Internet Service Provider (ISP). This is not infallible but pupils who deliberately try to access filtered material or bypass the filtering service will have their Internet access suspended.
    b. To help protect our students we also use Impero to monitor the use of our computers and Lightspeed to filter the internet use. The Online Safety Lead will be notified when a student uses a school computer to search for concerncing content which could indicate they are a risk to themselves or others.
4. The school email service can be used for personal use but the rules given below on email use must be followed.
5. Misuse of the Internet will result in the suspension of Internet access for a fixed period of time.
6. Pupils should not access website guestbooks, forums or chat rooms due to the unregulated nature of the content, unless there is clear educational value and a member of staff is aware of the activity.
7. If inappropriate material is accessed accidentally, users should immediately report this to a member of staff so that this can be taken into account in monitoring.

A summary of unacceptable usage:

Users shall not use the school Internet system to:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

    - pornography (*including images, video as well as explicit animation and textual descriptions*)
    - promoting discrimination of any kind (*including material that promotes intolerance on the basis of gender or sexual orientation*)
    - promoting racial or religious hatred
    - promoting illegal acts
    - promoting drugs and substance abuse (i*ncluding web sites that promote the use, manufacture and distribution of illegal drugs, as well as sites that promote the abuse of legal substances such as prescription drugs or the sale of alcohol to minors*)
    - graphic portrayal of violence, as well as sites that promote violence or self-endangerment, or contain instructions for making weapons of violence or the sale of such weapons
- Access web-based chat sites that allow users to make contact with individuals in the outside world without providing sufficient safeguards and protection to young people
- Access web-based email services, other that the service provided by the school
- Access sites offering Internet-based SMS messaging services
- Visit sites that might be defamatory or incur liability on the part of the school
- Upload, download, or otherwise transmit (*make, distribute or distribute*) commercial software or any copyrighted materials belonging to third parties outside the school
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (*sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion*) that substantially hinders others in their use of the Internet.
- Solicit, represent personal opinions or reveal confidential information or use it in any other way that could reasonably be considered inappropriate
- Access social media sites or apps, online gaming, chatrooms, newsgroups or any other website of this kind.
- Access the internet via personal devices such as mobile phones, smart watches or tablets (with the exception of students in the sixth form)

Additional Guidance on unacceptable usage

1. **Personal Safety:**
    a. Users will not e-mail personal contact information about themselves or other people. Personal contact information includes your address, telephone, school address, work address, etc.
    b. Users should not access or contribute to online forums as these are often unregulated.
    c. Pupil users should promptly disclose to a member of staff or other school employee any message they receive that is inappropriate or makes you feel uncomfortable.
2. **Illegal Activities:**
    a. Users will not attempt to gain unauthorised access to The FH School Network or go beyond their authorised access. This includes attempting to log-on through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".
    b. Users will not attempt to bypass the ISP filtering system. Such attempts will result in a permanent ban of Internet access
    c. Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
3. **System Security:**

a. Users are responsible for their individual user area and should take all reasonable precautions to prevent others from being able to use it. Under no conditions should users let any other pupil know their password.
b. Users will immediately notify a teacher or the system administrator if they have identified a possible security problem. Users MUST NOT go looking for security problems because this will be construed as an illegal attempt to gain access.
c. Users will avoid the inadvertent spread of computer viruses. Unchecked floppy disks and USB flash/pen drives must not be used and email attachments that are suspect or from unknown sources should not be opened.
d. Users will not download computer programs or files from the Internet without permission from a member of staff.
e. Users will not try to load computer programs onto the FH School Network or attempt to run programs that are not accessed through the Start Menu or Desktop screen.

4. **Inappropriate Language:**
   a. Restrictions against inappropriate language apply to public and private email messages, file names, the content of files and material posted on Web pages.
   b. Such inappropriate language includes obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
5. **Email misuse:**
   a. Users will not email information that could cause damage or a danger of disruption.
   b. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by someone to stop sending them messages, then they must stop.
   c. Users will not knowingly or recklessly email false or defamatory information about a person or organisation.
   d. Users will not forward an email that was sent privately without permission of the person who sent the message.
   e. Users will not email private information about another person.
   f. Users will not email chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
   g. Users will not use email in lessons without permission from the member of staff taking the lesson.
6. **Misuse of resources**:
   a. There are only a limited amount of computers available outside lesson times. Priority will always be given to uses who need to use the computers for educational and careers purposes and users must use the Internet only for educational and career development.
   b. Users will avoid unnecessary printing. A record of all printing is logged automatically by the Network. Users will be responsible for monitoring their printer credits using the Status Manager. Unnecessary printing will result in printer credits not being renewed.
   c. Accessing and playing games via the Internet is not allowed. A limited number of games do have some significant educational value and these listed 'games' are the only ones users are permitted to access.
   d. Running non-educational files on the network - users should not play non-educational multi-media such as MP3 or video clips. Bringing such files into school (*on USB flash drives or as email attachments etc.*) is not permitted.
   e. For copyright reasons, users must not store or download commercial music of video files anywhere on the school network.
   f. Shared areas on the school network are for transferring files and users are responsible for their removal when they are no longer needed. If users place inappropriate files in a shared area then then their network access is liable to be suspended.

g. Listening to online radio broadcasts or watching website video clips online slows the whole network. Unless this is for educational reasons and permission has been given by a member of staff, this is not allowed.

7. **Monitoring of the network.**
    a. Pupil users should expect only limited privacy in the contents of their personal files on the FH School Network.
    b. Routine maintenance and monitoring of files stored on the FH School Network may lead to discovery that users have violated this Policy or the law.
    c. Routine monitoring of user logs, user files and the screens of pupils using the Internet may lead to discovery that users have violated this Policy or the law.
    d. An individual search will be conducted if there is reasonable suspicion that users have violated this Policy. The investigation will be reasonable and related to the suspected violation.
    e. Parents have the right at any time to request to see the contents of pupil email files, both sent and received.
8. **Policy violations.**
    a. FH School will co-operate fully with local, or government officials in any investigation related to any illegal activities conducted through the FH School Network.
    b. Misuse of the Internet or email will result in user access to these facilities being suspended. The length of time the suspension will be enforced for will be dealt with on a case by case basis.
    c. Details and/or printouts of any unacceptable material or internet access may be posted home to parents/guardians.
    d. Users are responsible for the contents of their user area.

Education of students, staff and parents regarding online safety

Students

Students will be educated on Online Safety in the following ways:

- Assemblies and tutor time activities
- In lessons such as RSE (Relationships and Sex Education) and ICT which will cover how to remain safe online and how to use new technologies appropriately
- Students will be guided by teachers in lessons when ICT is used to facilitate learning across the curriculum. This could be carried out in a number of ways, such as teachers providing websites that are appropriate to access for the lesson being studied or helping students to understand what sources of information are regarded as acceptable.
- Students with SEN and disabilities will receive this information in a way that meets their needs, in some situations they may be be educated on online safety through 1:1 support.

Staff

- Staff will receive Online Safety training as part of their annual safeguarding update. This will be led by the Online Safety Lead for the school.
- All new staff will receive Online Safety training as part of the safeguarding training offered during their induction.
- Staff will be sent regular updates about current Online Safety issues or new Apps and websites that they need to have an awareness of.
- The Online Safety Lead will receive regular training and updates through attendance of official training schemes.

- The Online Safety Lead will provide assistance, support and training to staff members at their request or as required

Parents

- Parents will have access to information on Online Safety through channels such as the school website, letters home and newsletters.

Key members of staff involved in ensuring the Online Safety is followed:

- Miss Hankers
  Deputy Designated Safeguarding Lead / Online Saftey Lead
  chankers@farlingaye.suffolk.sch.uk

- Mrs Gilmour
  Desiganted Safeguarding Lead / Deputy Head Teacher
  lgilmour@farlingaye.suffolk.sch.uk

- Mr Aldridge
  ?????
  daldridge@farlingaye.suffolk.sch.uk

Appendix A

Our School

Online Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the online safety Rules have been understood and agreed.

Pupil:	***Form:***
Username if you know it:	

Pupil's Agreement

- I have read and I understand the school online safety Rules.
- I will use the computer, network, mobile phones, Internet access, Social networking sites and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil full names.

Parent's Consent for Internet Access

I have read and understood the school online safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***
Please print name:	

Please complete, sign and return to the school