E-Safeguarding Policy

This policy is to be read in conjunction with the following other school policies:

- **Safeguarding Policies**
- **Acceptable Use Policy (staff)**
- **Acceptable Use Policy (students)**
- **Induction Policy**
- **Health and Safety Policy**
- **Data Protection Policy**
- **Code of Conduct**
- **Anti-bullying Policy**
- **Disciplinary Policy**
- **Whistleblowing Policy**

Policy Produced: Autumn 2012

Policy Reviewed: Autumn 2014; Spring 2015; Spring 2016; Spring 2017; Spring 2018, Spring 2019, Autumn 2020, Autumn 2021; Autumn 2022; Autumn 2023

Date of next review: Autumn 2024
Policy Writer: Jim Weller

Contents

1) Policy Introduction

ICT (Information and Communication Technology) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the

constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites
Learning Platforms and Virtual Learning Environments
Email and Instant Messaging
Chat Rooms and Social Networking
Blogs and Wikis
Podcasting
Video Broadcasting
Music Downloading
Gaming
Mobile/ Smart phones with text, video and/ or web functionality
Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.
At Frederick Holmes School we understand the responsibility to educate our pupils on eSafeguarding issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, whiteboards, digital video equipment, etc.)

As eSafeguarding is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafeguarding co-ordinator in our school is **Jim Weller**. All members of the school community have been made aware of who holds this post. It is the role of the eSafeguarding co-ordinator to keep abreast of current issues and guidance through organisations such as Hull Local Authority, CEOP (Child Exploitation and Online Protection), Childnet and YHGfL (Yorkshire and Humber Grid for Learning).
Senior Management and Governors are updated by the Head/ eSafeguarding co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.
This policy, supported by the schools acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

This eSafeguarding policy, created under guidance of the YHGfL criteria, has been produced for a number of key reasons:

- To set out the key principles expected of all members of the school community at Frederick Holmes School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Frederick Holmes School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

2) Scope of Policy

- This policy applies to the whole school community including the Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.
- Frederick Holmes School's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other eSafeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of school.

3) Review and Ownership

- The school has appointed an eSafeguarding coordinator who will be responsible for document ownership, review and updates.
- The eSafeguarding policy has been written by the school eSafeguarding Coordinator and is current and appropriate for its intended audience and purpose.
- The school eSafeguarding policy has been agreed by the senior leadership team and approved by governors.
- The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The School has appointed a member of the governing body to take lead responsibility for eSafeguarding.
- All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff. The school staff are expected to read and sign the eSafeguarding policy on an annual basis.

4) Communication Policy

The senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.

- The eSafeguarding policy will be provided to and discussed with all members of staff formally.

- An eSafeguarding or eSafety module will be included (where appropriately) in the PSHE (Personal, Social and Health Education), Citizenship and/or Computing curricula covering and detailing amendments to the eSafeguarding policy.
- The school will annually review the eSafeguarding policy.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used
- Internet Safety posters are prominently displayed around the school

5) Roles and Responsibilities

Responsibilities of the senior leadership team

- The headteacher is ultimately responsible for eSafeguarding provision for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator.
- The headteacher and senior leadership team are responsible for ensuring that the eSafeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal eSafeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the eSafeguarding Coordinator.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

Responsibilities of the eSafeguarding Coordinator

- To promote an awareness and commitment to eSafeguarding throughout the school
- To be the first point of contact in school on all eSafeguarding matters
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the designated eSafeguarding governor Jamie Lewis
- To communicate regularly with the senior leadership team
- To create and maintain eSafeguarding policies and procedures
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that eSafeguarding education is embedded across the curriculum
- To ensure that eSafeguarding is promoted to parents and carers

- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident
- To ensure that an eSafeguarding incident log is kept up to date
- To monitor Smoothwall through daily reports and maintain a record/ manage any filtering issues/ potential breaches/ inappropriate web searches on a weekly basis

Responsibilities of teachers and support staff

- To read, understand and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the eSafeguarding coordinator
- To develop and maintain an awareness of current eSafeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils (where appropriate) are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of pupils (where appropriate)

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices
- To know and understand school policies on the taking and use of mobile phones
- To know and understand school policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- Where possible pupils to be fully aware of research skills and of legal issues relating to electronic content such as copyright laws
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to

- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss eSafeguarding issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting eSafeguarding
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the acceptable use policy (students)

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the eSafeguarding co-ordinator in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy

Responsibilities of the Designated e-Safeguarding Lead

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose
- To make referrals to appropriate agencies if a pupil is at risk of harm.

6) Cyberbullying

Frederick Holmes School has a duty to protect pupils and staff from online activities that are harmful and damaging and which can, in some circumstances, constitute a criminal act. Cyberbullying - the use of new and emerging technologies to cause harm or distress to another person – poses a growing challenge and the School

possesses a clear framework of guidelines in this area including curriculum taught topics.

Key advice to pupils on how to deal with cyberbullying:

- Do not be enticed into compromising messages/posts
- Always respect others: think about what you say online and what images you send/post
- Remember that anything you publish online can be made public very quickly and you will never be sure who may have seen it. Once something is posted, presume it is permanently public
- Treat your password carefully – never share it with anyone and only give personal information like a mobile phone number or email address to trusted friends
- Learn how to block or report online bullies or anyone behaving badly
- Don't retaliate or reply to nasty messages
- Save the evidence – text messages, online conversation, pictures etc
- If you see cyberbullying going on, then support the victim and report it
- Avoid using anonymous websites

NB: if you have any concerns relating to cyber-bullying, please speak at once to your class teacher or support staff. Alternatively you can speak to Mr Weller (E-safeguarding Officer). Reporting slips are available from the class teacher and on the e-file.

Key advice for parents on how to deal with cyberbullying:

- Model positive online behaviour: it's important that they know how to act safely and responsibly online and are aware of what content is acceptable and unacceptable to post or share
- Talk to your child and understand how they are using the internet and their phone
- Use safety tools and parental controls: http://www.saferinternet.org.uk/advice-andresources/parents-and-carers/parental-controls outlines how you can turn on 'parental filtering' in the home. Some providers can offer more sophisticated services than others, but all internet providers are obliged to offer a parental filtering option. Your children's iPads are filtered whilst they are in school, but this does not apply in your homes
- Remind your child not to retaliate to any cyberbullying
- Work with the school to resolve the issue if other pupils are involved
- Keep any evidence of cyberbullying – emails, online conversations, texts, screenshots of sites/chat messages – and try and include time/date where possible
- Report the cyberbullying: contact the service provider (e.g. the website, gaming site or mobile phone company) to report the user and if possible to remove the content. Contact the School so it can take action if it involves other pupils
- If the cyberbullying is serious and a potential criminal offence has been committed then contact the police.

Key advice to protect staff:

- Keep all passwords and login details secret and ensure you lock your computer or office if away from your desk
- Make sure you understand how to secure any websites or social networking services you use
- Always think carefully before you post and don't post any information (photos, videos, comments) publicly online that you wouldn't want employers, colleagues, pupils or parents to see. Just because a profile might be set to 'private' it doesn't mean that someone else can't copy or share it without your knowledge
- Also consider if it could bring you, the School's or someone else's reputation into disrepute: posting something inappropriate, obscene or threatening online could lead to criminal, civil and/or disciplinary action
- Do not use your own personal devices or personal social networking profiles to contact pupils or parents
- Ensure that the School's rules and policies regarding the use of technologies by pupils and staff are enforced. Make sure you read and understand the School's Acceptable Use Policy.
- Do not personally retaliate to any incidents which involve yourself or other members of staff
- Always report any incidents of cyberbullying witnessed (either of yourself or other staff members) in a timely manner
- Make sure you save and keep any evidence of cyberbullying, e.g. screenshots. Where possible record times, dates and user names

7) Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/ Safeguarding Co-ordinator). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils. Reports are produced on a daily basis.

8) Sexual Abuse and Sexting

Sexual abuse is not solely a physical issue that schools must deal with. It can also occur online. Children and young people at Frederick Holmes School are supervised in their use of the internet and also receive guidance for managing their online behaviours and staying safe through the e-safety curriculum.

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using any device that allows the sharing of media or messages including tablets, mobiles and laptops.
When an incident involving youth produced sexual imagery comes to the attention of the school:

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent work with the young people involved (if appropriate)

- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

Children and young people, where appropriate, are taught about the dangers involved with sexting as part of the e-safety curriculum.

9) Managing digital content

Using images, video and sounds

Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done annually or as part of the home-school agreement on entry to the school.

On the school website
In display material that may be used around the school
In display material that may be used off site
Recorded or transmitted on a video or via webcam in an educational conference
On social media including Facebook and Twitter

- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

10) Learning and Teaching

- We will provide a series of specific eSafeguarding-related lessons in appropriate classes as part of the Computing curriculum.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions

may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Where appropriate, some pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff training

- As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas.
- Regular sessions will be delivered in-house by the eSafeguarding co-ordinator to ensure staff remain aware of e-safety issues and protocols.
- Staff receive support materials to aid in the delivery of e-safety topics.
- Briefing documents are available (and updated when necessary) in the Safeguarding files for each class and on the eFile.
- All staff are directed to watch a cyber security video on an annual basis
- All staff receive monthly Boxphish training focusing on E-Safety and Cyber security.

11) Managing ICT systems and access

- The school, and managed service will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems is based upon a 'least privilege' approach.
- Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software are kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and is kept active and up to date.

- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- Some users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID and password. They will abide by the school AUP at all times.

12) Passwords

All staff are given a username to access both the school network and also email. They are expected to create their own passwords when prompted. Some pupils in the school are given their own unique usernames and passwords for logging on. If appropriate they may change these passwords but should inform their teacher so that copies of the passwords can be locked securely away. For other pupils there will be a generic password due to particular access issues. A secure and robust username and password convention exists for all system access. (email, network access, school management information system).

- All staff have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users are prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.

13) Emerging technologies

At Frederick Holmes School we want to give all pupils opportunities to use new technologies no matter how limited they may be with regards access ability. Therefore we constantly research emerging technologies and assess suitability as learning tools.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level.
- Emerging technologies can incorporate software and/or hardware products.
- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

14) Filtering internet access

We filter internet activity for two reasons:

Firstly so that (as much as possible) children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
Secondly so that (as much as possible) the school has mitigated any risk to the children/young people, and thereby reduces the liability to the school by making reasonable endeavours to ensure safety.

- The school uses a filtered internet service. The filtering system is provided by East Riding Council who have installed and manage Smoothwall.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents are documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such

incidents to appropriate agencies including the filtering provider, the local authority, CEOP (Child Exploitation Online Protection) or the IWF (Internet Watch Foundation).

- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

The school uses Smoothwall to monitor internet usage. Reports are delivered daily to the Assistant Head Teacher and Head Teacher who check, whether there have been any breaches/ inappropriate use of the internet by both pupils and staff members. A separate report is also received on a daily basis outlining whether any breaches around suicide have been recorded. Staff and pupils are questioned as to their use of the internet and any sites which have been identified to be questionable are reported to East Riding Council who will then ensure they are blocked. Staff are given regular reminders and training re their conduct using school internet and are aware that inappropriate usage could lead to disciplinary procedures. It must be recognised that no monitoring can guarantee to be 100% effective.

Areas which must be filtered and monitored are:

- Discrimination
- Drugs/Substance abuse
- Extremism
- Malware/Hacking
- Pornography
- Piracy and copyright
- Self-harm
- Violence

15) Internet access authorisations

- All parents will be required to sign an agreement form prior to their children being granted internet access within school.
- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- Where appropriate, pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.

16) Email

Email usage

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Pupils must not reveal personal details of themselves or others in email communications.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Pupils and staff should never open attachments from an untrusted source but should consult the eSafeguarding co-ordinator first.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- All pupils with active email accounts are expected to adhere to the generally accepted rules of etiquette; particularly in relation to the use of appropriate language. They should not reveal any personal details about themselves or others in email communication or arrange to meet anyone without specific permission.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately (as per Whistleblowing protocols)
- All email users within school should report any inappropriate or offensive emails through the incident-reporting mechanism within school.
- Pupils must immediately tell the eSafeguarding co-ordinator if they receive any inappropriate or offensive email.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.
- Emails sent to external organisations should be written carefully and, if appropriate, authorised before sending to protect the member of staff sending the email.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.
- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system can be monitored and checked.
- Some pupils will be allocated an individual email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.

- Staff and pupils are not permitted to access personal email accounts during school hours unless this is part of the lesson.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. An audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers, as approved by the senior leadership team.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

17) Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the school website and postings should be approved by the headteacher before publishing.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils will only use their first name when creating publicly-accessible resources. They will however be encouraged to create an appropriate nickname.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

Twitter and Facebook

Social Networking – there are many social networking services available; Frederick Holmes is fully supportive of Social Networking as a tool to engage and collaborate with pupils and engage with parents and the wider community. At Frederick Holmes School we use Twitter as a broadcast service, which is a one-way communication method in order to share school information with the wider community. No person will be 'followed' or 'friended' on this service and as such no two-way communication will take place.

The school has a group Facebook page. Any posts are monitored by the Assistant Head and access to the site is strictly by invitation only.

18) Mobile phone usage in schools

General issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of personal devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity unless authorised by the Head Teacher.
- Staff will use a school phone where contact with pupils, parents or carers is required. The SLT have shared school mobile numbers for out-of-hours emergencies with all staff and parents.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, they may use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

19) Data protection and information security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Alt-Del) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- All documents sent to the photocopier will be retained until a password is inputted on the device.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, remote access over encrypted tunnel. Staff will not take data off site using memory sticks.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not be left in cars or unsecure locations.

20) GDPR

The General Data Protection Regulation (GDPR) will come into effect on the 25th May 2018 and will cover all the countries in the EU and will be adopted by the UK. It is heavily based on the Data Protection Act 1998 but will lead to schools having to refine their approach to Data Protection. At its heart it changes the importance of Data Protection and emphasises the schools' accountability. Making Data Protection important means that Frederick Holmes School will employ 'Privacy by Design' – thinking about how the school uses data in everything it does. Policies and procedures will be in line with the expectations of the Local Authority.

21) Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

References

Particularly for Parents and Children

Yorkshire and Humber Grid for Learning (YHGfL) www.yhgfl.net
Excellent resources for understanding the need for safeguarding

Think U Know? www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

National Action for Children (NCH) www.nchafc.org.uk/itok/
Parent's Guide on Internet usage

Bullying Online www.bullying.co.uk
Advice for children, parents and schools

FKBKO - For Kids By Kids Online www.fkbko.co.uk
Excellent Internet savvy for kids; KS1 to KS3

Parents Information Network (PIN) www.pin.org.uk
Comprehensive guidelines on Internet safety

Parents Online www.parentsonline.gov.uk/2003/parents/safety/index.html
Interactive learning and safety advice, excellent presentation for parents.

Kidsmart www.kidsmart.org.uk
An Internet safety site from Childnet, with low-cost leaflets for parents.

Family Guide Book (DCSF recommended www.familyguidebook.com
Information for parents, teachers and pupils

NCH Action for Children www.nchafc.org.uk
Expert advice for children, young people and parents.

Safekids www.safekids.com
Family guide to making Internet safe, fun and productive

Particularly for Schools

Associations of Co-ordinators of IT (ACITT)
Acceptable use policy for the Internet in UK Schools, original straightforward text.
www.g2fl.greenwich.gov.uk/acitt/resources/assoc/aup97.doc

NAACE / BCS www.naace.org (publications section)
A guide for schools prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

DCFS Superhighway Safety http://safety.ngfl.gov.uk
Essential reading, both Web site and free information pack. Telephone: 0845 6022260

KS2 Internet Proficiency Scheme
www.becta.org.uk/corporate/corporate.cfm?section=8&id=2758
A Becta, DCFS and QCA pack to help teachers educate children on staying safe on the
Internet

Internet Watch Foundation - www.iwf.org.uk
Invites users to report illegal Web sites

Data Protection www.informationcommissioner.gov.uk/
New Web site from the Information Commissioner

Kent Web Skills Project www.kented.org.uk/ngfl/webskills/
Discussion of the research process and how the Web is best used in projects.

Click Thinking: Scottish Education Department
www.scotland.gov.uk/clickthinking
Comprehensive safety advice

Kent ICT Security Policy www.kent.gov.uk/eis (broadband link)
An overview of the need to secure networks with Internet access.

Copyright www.templetons.com/brad/copymyths.html
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.

Internet Users Guide www.terena.nl/library/gnrt/
A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web.

Alan November – The Grammar of the Internet www.edrenplanners.com/infolit/
Article explaining how to evaluate Web sites and information

DotSafe – European Internet Safety Project
http://dotsafe.eun.org/
A comprehensive site with a wide range of ideas and resources, some based on Kent work.

Cybercafe http://www.gridclub.com/home_page/hot_headlines/cyber.shtml
Internet proficiency through online games for KS2, with a free teacher's pack.

Appendix 1

Safer Working Practice Guidelines: Online lessons

Summary

Since schools around the country have closed due to the coronavirus pandemic, school leaders and teachers have been looking at innovative ways to allow them to teach pupils while everyone is staying at home. This helps to maintain a sense of structure to children's days and allows them to keep in contact with their teachers and class mates. These innovative lessons enable teachers to continue to engage pupils and consolidate their existing skills and knowledge.

Posting pre-recorded lessons online and hosting video conferencing have become a popular way of delivering teaching. However, it is vital that these services are used safely and securely by teachers and pupils.

Frederick Holmes School is committed to ensuring pupils and staff stay safe online. In order to achieve this, the following guidance outlines necessary protocols as well as an outline of what security settings are available and how to use them.

The two ways of teaching pupils online

Passive
Teacher posts activities and student posts responses. These are often filmed by teachers in advance and posted online - e.g. online tutorials via YouTube, on GSuite or a learning portal. Teachers may also consider Podcast/voice tutorials.

Interactive or live
Pupils and staff connected in the same service at the same time – e.g. live video and audio. For example, Zoom conferencing (or other similar

technology). This will **not** be the most appropriate approach for children and young people at Frederick Holmes School.

Responsibilities

Headteachers must:

- Develop and agree a whole school policy for online learning, deciding whether to use passive and/or interactive lesson formats. They must ensure any platforms, apps, technology used by teachers are safe, secure and age appropriate.
- Authorise the planning and implementation of virtual classrooms (passive or interactive);
- Ensure they monitor the content of virtual/online lessons (passive or interactive);
- Safeguard staff from potential allegations by ensuring live lessons are recorded and/or a second member of staff is present. However, recordings must not be used for monitoring teacher performance;
- Ensure parents provide written consent for their child to join interactive lessons, making them aware that the lessons may be recorded by the teacher and the reasons for this;
- Ensure all staff hosting online lessons (passive or interactive) are happy and confident to do so. They should receive appropriate technical and safeguarding guidance and support.

Teachers must:

- Demonstrate consistently high standards of personal and professional conduct, as referenced in the Teacher Standards when hosting online lessons (passive or interactive);
- Gain the authorisation of the Headteacher before producing/hosting passive and/or interactive lessons;
- Follow the agreed protocols stated below.

Protocols applicable to both passive and interactive online lessons

- Teachers must only use apps, platforms and technology that have been authorised by the Headteacher.
- Teachers must wear suitable clothing and should be in a neutral area where nothing personal or inappropriate can be seen or heard in the background.
- Teachers must always make sure the platform they are using is suitable for the children's age group and agreed by the Headteacher.
- Teachers must set up school accounts for any online platforms they use and never use their personal accounts.

- Teachers should check the privacy settings.

Protocols specific to <u>interactive</u> online lessons

- Teachers must not deliver lessons to pupils who are located in bedrooms. If this happens, the teacher must make contact with the parent and them to ensure the pupil moves to a communal living area or leaves the lesson.
- Teachers must not deliver interactive lessons to just one child unless:
a) a parent is present with the child and/or
b) a colleague is 'virtually' present with the member of staff.
- In order to safeguard teachers from potential allegations, another colleague should be present and/or the lesson must be recorded (see Headteacher responsibilities section);
- Pupils must not **record** the virtual meeting as this could be shared without the teacher's consent. Details of how to restrict this can be found using the following link: https://support.zoom.us/hc/en-us/articles/201362473-Local-Recording
- Teachers must only deliver lessons during normal school opening hours.

<u>Keeping safe in an online classroom</u>

Zoom (or other similar technology) conferences can be accessed by unauthorised visitors. There have been cases (known as 'zoombombing') in which unauthorised visitors have displayed/demonstrated inappropriate actions/content. In order to prevent this happening, teacher must:

- **'Lock' classrooms** - If your class has started and all your pupils have arrived, you must **lock your classroom**, so that no one else can join.
- **Create virtual waiting rooms** - This feature of Zoom lets people who want to join a class to be held in a virtual waiting room before being let into the classroom. This allows you to check who each person is before allowing them entry. There's also a setting to allow known students to skip the waiting room, so you don't have to manually allow 30 pupils every time.
- **Screen sharing** - Make sure your pupils don't take control of the screen and prevent them from sharing random content by **limiting screen sharing**, so only you as the teacher (host) can present to the class.
- **Private messaging** - Safeguard pupils by **stopping private messaging** between them, so they can't talk to one another without your knowledge.

- **IDs/Passwords** - Teachers must use **random meeting IDs** and **password protect all classrooms**.

Technical guidance on how to action the above can be found by clicking on: https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/

Frederick Holmes School has a duty of care to all employees. Teachers should speak to a member of the school's senior leadership team if they have any questions/concerns about delivering lessons online.

This guidance has been produced so that Headteachers and employees follow safer working practices.

References

https://www.childrenscommissioner.gov.uk/coronavirus/keeping-classrooms-safe-online/