WIRRAL

3

Meadowside e-Safety Policy

Reviewed and Updated July 2021 K.Charmley

Reviewed and Updated October 2019 K.Charmley
Revised May 2018
Revised/updated May 2011, 2012, 2014, 2015, 2016, 2017 and again Dec 2017 C. Hughes
Adopted June 2010

Agreed:	**Ratified:**
Governors' Policies meeting	15th July 2021
Finance/H&S/Premises: 19.6.18	Full Governing Body 28.6.18
Finance/H&S/Premises: 13.6.17	Full Governing Body 29.6.17
Finance/H&S/Premises: 14.6.16	Full Governing Body 23.6.16
Finance/H&S/Premises: 16.6.15	Full Governing Body 25.6.15

Inspiring Brighter Futures

Intent

The E-safety policy is designed to ensure that technology (devices and the internet) is used in the correct and most beneficial way to pupils and staff, whilst making safety and security top priority (KCSIE 2020) particularly relating to online activity.

Meadowside School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.
The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.
The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

Voyeurism (Offences) Act 2019

The UK General Data Protection Regulation (UK GDPR)

Data Protection Act 2018

DfE (2021) 'Harmful online challenges and online hoaxes'

DfE (2021) 'Keeping children safe in education 2020'

Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

DfE (2019) 'Teaching online safety in school'

DfE (2018) 'Searching, screening and confiscation'

National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'

UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

DfE Sexual violence & sexual harassment between children in schools" Sept 2021

Principles

The school has appointed the Head Teacher and Assistant Head (Innovation) as the eSafety co-ordinators. Our e-Safety Policy has been written by the Subject Leader.

Use of Internet

Why is internet use important?

The 2014 National Curriculum for Computing requires learners to:

- *understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration*
- *understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct, and know how to report concerns*
- *understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to report a range of concerns*

The purpose of internet use in school is to raise educational standards, to promote learner achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning, both in school and in some situations for home learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for learners who show a responsible and mature approach to its use. Our school has a duty to provide learners with quality internet access

Learners will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How does internet use benefit education?

Benefits of using the internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between learners world-wide
- Access to experts in many fields for learners and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;

- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DFE

How Can Internet Use Enhance Learning?

- The school internet access will be designed expressly for learner use and includes filtering appropriate to the age and skills of learners
- Learners will be taught and supported as to what internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide learners in on-line activities that will support learning outcomes planned for the learners' age, skills and maturity
- Learners will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and selection of suitable and reliable information from trustworthy sources.
- Internet gives wider scope of resources and opportunity for Home Learning as necessary (as seen more recently with COVID 19)

Use of Devices

- Meadowside offers staff and pupils a range of technology devices to aid teaching and learning across the curriculum.
- We endeavour to have equipment kept up to date and fully functional.
- Safety of equipment is a priority and staff/pupils know they must report any faults or damaged equipment.

Implementation

Authorised Internet Access

- The school will maintain a current record of all staff and learners who are granted internet access
- All staff must read and sign the 'Acceptable ICT and Computing Use Policy Agreement' (AUP) before using any school ICT resource
- Parents will be informed that learners will be provided with supervised internet access
- Parents will be asked to sign and return a consent form for learner access
- Learners must apply for internet access individually by agreeing to comply with the Responsible Internet Use statement- AUP
- Staff must agree to support learners in complying with the Acceptable ICT and Computing Use Statement.
- The ICT and Computing Subject Leader will keep a log of all internet user account names and users.

World Wide Web

- If staff or learners discover unsuitable sites, the URL (address), time, content must be reported to the Head Teacher and recorded in the eSafety log (held by Computing Lead).
- School will ensure that the use of internet derived materials by learners and staff complies with copyright law.
- Learners should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- A YouTube advice poster should be displayed in every classroom, reminding learners to ask first and detailing specifically what constitutes unsuitable content.
- A 'Where to get help' poster should be displayed in every classroom, in line with DfE recommendations, so pupils are always aware of how to gain help in ESafety matters.

Email

- Learners may only use approved e-mail accounts on the school system
- Learners must immediately tell a teacher if they receive offensive e-mail
- Learners must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations by learners should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

- For learning purposes the school will use anonymous email accounts including 'couldbeanyone@meadowsideschool.com' and 'stranger@gmail.com' to teach pupils safe and potentially unsafe email communication. This can also be taught through interactive 'mock' emails in purple mash

Password Protection – School Network and Gmail

- The ICT and Computing leader supports the management of passwords for staff and learners.
- Staff are encouraged to change their passwords on a regular basis.
- Use of generic passwords must be strictly controlled by the ICT and Computing leader. Generic passwords will not be used for pupil school network accounts or email.
- Learners must not disclose passwords to other learners.

Social Networking

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- The school has a Facebook page and a Twitter page, managed by the Assistant Head. They are intended for promotional purposes only, not for communicating directly with individuals. Any contact made via these sites will be entirely professional.
- Learners will be advised never to give out personal details of any kind which may identify them or their location
- Learners **and staff** should be **advised** not to place personal photos on any social network space, particularly if privacy settings are not secure.
- Learners should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Learners should be encouraged to invite known friends only and deny access to others
- Staff are actively discouraged from having public profiles and prohibited from having current or school age learners as 'friends'. This applies to learners until they reach age 25.
- Staff are advised that they put themselves at risk if they have Facebook accounts that have ANY links with their working life-comments, friends, photos etc.
- All staff sign a specific policy on the use of Social Networking sites.

Filtering

The school will work in partnership with the Local Authority, and RM Safety Net filter to ensure filtering systems are as effective as possible.

Video Conferencing/Facetime

- Learners should ask permission from the supervising teacher before making or answering a videoconference/Facetime call
- Videoconferencing will be appropriately supervised for the learners' age
- Camera access is restricted on the ipads and requires a passcode within settings to enable it.

USB memory sticks & other Portable Data Storage Devices

- Staff to consider what data should be stored on USB sticks/other data storage devices. Data on USBs should be encrypted if it contains information about pupils.
- Sensitive data should be password protected, a feature available in most Office documents.
- Learner-use school USB sticks to remain in school under the supervision of the ICT and Computing leader.
- Learners should not use USB sticks from home unless arranged with the ICT and Computing leader and the USB stick checked for viruses before use.

iPads

- Only the Assistant Head Teacher (Innovation), Computing Lead and the appointed TA ICT Support staff member has the password to access paid Apps for the iPads.
- All iPads require a password to download even free Apps.
- All staff will check that selected Apps do not lead to unsuitable sites/adverts that may intend to indoctrinate pupils with religious or political views.
- iPads monitored monthly for unauthorised downloads and content
- iPad checklist carried out monthly, by an appointed TA, checking settings and restrictions

Digital Cameras

- Staff to use school cameras or iPads to photograph learners.
- Staff must not use personal equipment to photograph learners without permission from the Head Teacher.
- Storage cards to be cleared when camera returned.

Web Cams

- Web cams can be used for use as a mouse alternative for those with physical access limitations. They must be disconnected when not in use. Camera Mouse software must be loaded to use them as mouse alternatives.
- The new laptops in the ICT and Computing trolley all have built in webcams. Learners will be supervised at all times when using the machines.

Storage of Photographs

- Photographs to remain on school premises (when practicable –ie off site school trips – images only to be downloaded to school network/ school laptops.
- Staff (authorised by the ICT strategic leader) will assure that personal data including images is kept secure and is used appropriately, whether in school, taken off the premises or accessed remotely.
- Staff will use the P:/ Drive to store images for shared, school-only access.
- Photographs to be deleted when no longer required.
- Current school policy is adhered to regarding photographing & publishing images of learners, in line with LA guidance.
- School iPads are linked to a secure Dropbox cloud storage solution, with only staff having access to the username and password
- School staff iPads are to be password protected.

Mobile Phones & Other Hand Held/Communication devices

- Mobile phones & other hand held communication devices should not be used for personal use in the lesson or formal school time. Learners are asked not to bring in personal mobile phones unless they need to use one on LA transport. Such devices are handed in to School Office daily. Mobile phones should never be used on-site, when in sight of learners, regardless of time. Staff taking their own phones off site, with permission from the Head Teacher, should be mindful of using in front of learners, regardless of time.
- Mobile Phone – Bluetooth should be turned off or password protected.
- Sending of abusive or inappropriate messages is forbidden.
- Pupils will be taught the dangers of 'sexting' and its consequences
- Staff should not engage in sexting, being mindful of the damage to their reputation and professional persona.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Health & Safety/Safeguarding Officer and agreed by the governing body, before use in school is allowed.
- Handheld communications devices/ gaming consoles are not to be brought into school by learners without permission from the Head Teacher or Senior LeadershipTeam.
- Some learners bring electronic devices for use on LA transport journeys. Such devices are handed in to School Office daily.

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or learners' personal information will not be published
- The Head Teacher/Assistant Head (Innovation) will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Learners' Images and Work

- Photographs that include learners will not be used without permission
- Learners' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of learners are published on the school Web site.
- Work can only be published with the permission of the learner, where appropriate.

Monitoring & Resources

Information System Security

- School ICT and Computing systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly, as advised by the LA technician
- Security strategies will be discussed with the Local Authority, provided we buy into the SLA.
- Also see the use of 'USB memory sticks and other portable storage devices' section.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wirral Metropolitan Borough Council (despite providing the filter) can accept liability for the material accessed, or any consequences of internet access.
The school will audit ICT and Computing use to establish if the e-safety policy is adequate and that the implementation of the e-Safety policy is appropriate every 12 months.

YouTube

Access to YouTube is subject to an 'Ask First' policy. Learners are reminded at the time that no unsuitable material is to be accessed. Learners who have purposefully viewed inappropriate material will have YouTube use prohibited. This is in line with the Internet Acceptable Use Policy, which all staff must sign. Staff will ensure that video recordings made by pupils are not uploaded to YouTube under a personal OR school owned account.

Handling eSafety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff, Safeguarding officer or Head Teacher
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures
- Learners and parents will be informed of the complaints procedure

GDPR and internet use

School staff are required to take account of the regulations for protecting individuals' data. The GDPR came into effect on 25th May 2018 and all persons who process or control identifiable data, such as names, email addresses etc need to be mindful of who they share such information with.

All staff are required to carry out a risk assessment of their access to data off site, including the journey between home and school. Staff with access to school accounts on personal devices such as home computers, smart phones and tablets need to be mindful of where and how the data is accessed and protected.

Commented [PW1]: delete

Training

Learners

"Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum." KCSIE 2020

Pupils are taught about Esafety each year within their computing curriculum. As well as this, safeguarding and safety is also covered within PSHE and via Outside agencies (when possible) along with being embedded across the curriculum.

Staff

PREVENT Strategy

- Staff will all be 'Channel Aware', having undertaken the short training session and being certificated.
- Staff will report incidents of concern to the Head Teacher/Assistant Head Teacher (Innovation) and the incidents will be logged
- All staff (teaching & non teaching) are part of inset
- Supply staff must sign and adhere to the Social Network Policy and Internet AUP Outside agencies/LA
- Yearly review of training
- INSET – incorporating safeguarding as a high priority within the school

Governors

Outside agencies/LA
Yearly review of training

Parents

Sessions/workshops for parents

Communication of Policy

Learners

- Learners will be informed that internet use will be monitored. Visitors to the school, such as Outreach Primary Schools, will use the internet under close supervision.
- When accessing the internet in lessons, pupils will be regularly reminded within the lesson about suitable use of internet.
- Pupils will have Esafety lessons planned into each academic year.

Staff

- All staff will be given the School eSafety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The ICT and Computing Leader will manage filtering systems or monitor ICT use for the Senior Leadership Team and have clear procedures for reporting issues
- Induction for Supply Staff will include guidance on the school eSafety Policy.

Governors

- Acceptable Use Policy

Parents

- Parents' attention will be drawn to the School eSafety Policy in newsletters, the school magazine and on the school website.
- Parents provide written consent at Admission meetings.
- Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.
- Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

Parents' evenings / Events

Twilight training sessions

Newsletters / Magazine

Online resources / Homework /Remote Learning Support Team

Visitors

- Visitors to school will be informed about the eSafety policy at the reception desk
- Rules for visitors clearly displayed (i.e. use of mobile phone/camera/film equipment etc).

Rules for Visitors

- Only visitors authorised by the Head Teacher are granted use of any of the school's Information Communications Systems, including access to the internet.
- All visitors must work within the eSafety Policy- available in the School Office.
- Visitors will only use the school's internet/mobile communication devices/email with permission from the Head Teacher/Assistant Head Teacher (Innovation)
- Visitors will switch mobile phones and other hand held communication devices to silent/vibrate and not use these in lesson or formal school time in sight of learners.
- Mobile phone Bluetooth should be switched off.
- Sending of abusive or inappropriate messages/ images is forbidden.
- A Risk Assessment will be carried out by the Health & Safety Officer/ Safeguarding Officer/ Head Teacher before use in school is allowed.
- The use of photographic devices is forbidden in formal school time, without prior permission from the Head Teacher.

Impact

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects: RSE, Health education, PSHE, Citizenship, Computing. The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The Subject Leader is accountable for high expectation, planning, assessment, recording and reporting of pupil progress, liaising and moderating the planning and assessment in terms of fluency and independence

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's eSafety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems, (mobile phone, mobile communication devices, Facebook), use will always be compliant with my professional role.
- I understand that the school may monitor my professional information systems and internet/email use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission from the ICT leader.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding learners' e-safety to the school eSafety Coordinator or the Head Teacher, Child Protection Lead (Anti Radicalisation)
- I will ensure that any electronic communications with learners are compatible with my professional role.
- I will promote eSafety with learners in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for radicalisation, criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Printed: …… Date: ……

Accepted for school: ……

Capitals: ……

Learner AUP

eSafety Rules

All learners use ICT facilities including internet and email access as an essential part of learning, as required by the National Curriculum. Both learners and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Learner:	***Class:***

Learners' Agreement

- I have read and I understand the school eSafety Rules.
- I will use the computer, network, internet access 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 learner names.

Parent's Consent for Internet Access

I have read and understood the school eSafety 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 learners 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

Appendix A: eSafety Rules

eSafety Rules

These eSafety Rules help to protect learners and the school by describing acceptable and unacceptable computer use.

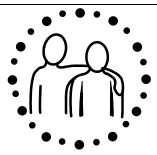
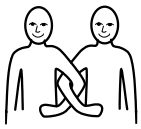
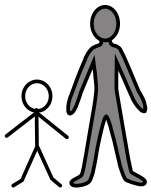
- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network, internet and email use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- Use for personal financial gain, gambling, political activity, radicalisation, advertising or illegal purposes is not permitted.

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

Appendix B: *Learner/ Learner AUP*

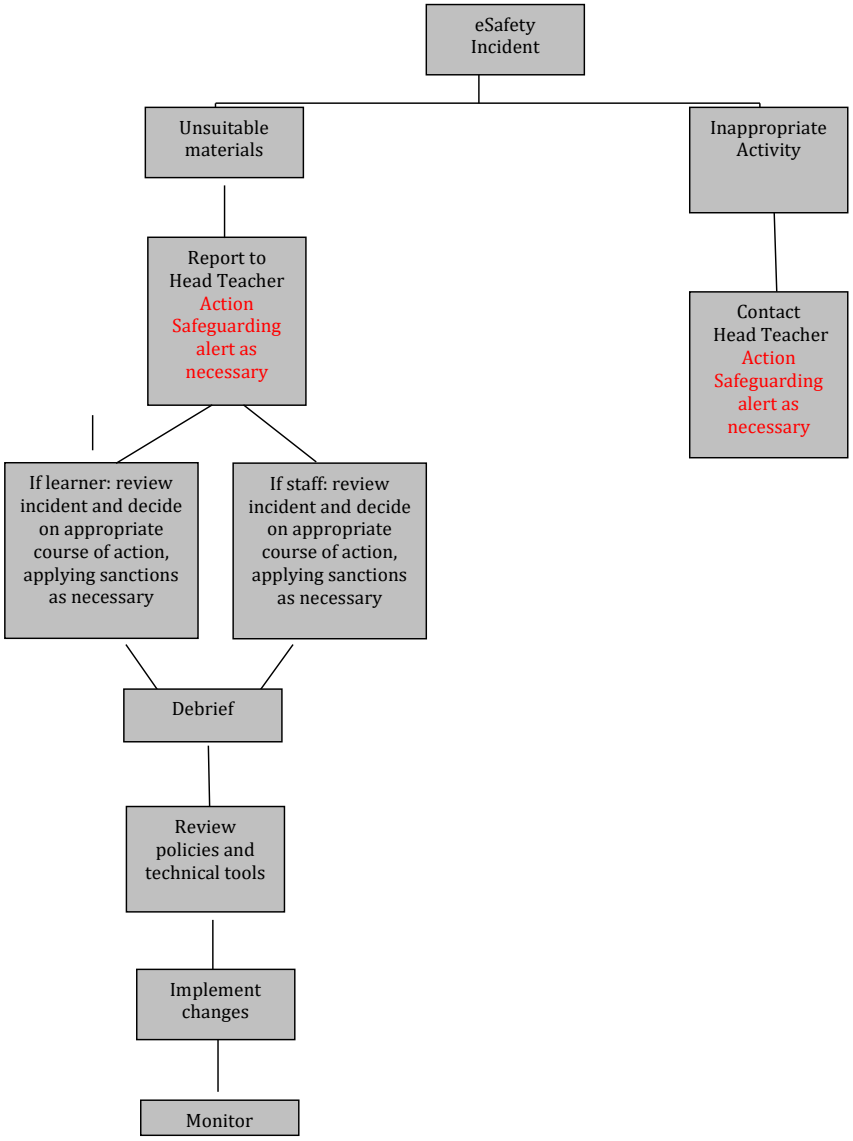
Think Before You Click

Use these rules to stay safe when using the School Information Communications Systems

S 	I will only click on icons and links when I know they are **safe**
A 	If I see something I don't like on the screen, I will always **alert** an adult.
F 	I will only send **friendly** and polite messages
E 	I will only use the internet, website, the webcam and **email** with an adult.

My Name
My Signature

Appendix C: Flowchart for responding to eSafety incidents



Appendix D: eSafety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the eSafety basics are in place.

Has the school an eSafety Policy that complies with CYPD guidance?	**Y/N**
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Learner Protection Teacher/Officer is:	
The eSafety Coordinator is:	
Has eSafety training been provided for both learners and staff?	**Y/N**
Is the Think U Know training being considered?	**Y/N**
Do all staff sign an ICT Code of Conduct on appointment?	**Y/N**
Do parents sign and return an agreement that their learner will comply with the School eSafety Rules?	**Y/N**
Have school eSafety Rules been set for learners?	**Y/N**
Are these Rules displayed in all rooms with computers?	**Y/N**
Is internet access provided by an approved educational Internet Service Provider and complies with DFE requirements for safe and secure access?	**Y/N**
Has the school filtering policy been approved by SLT?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Y/N**

Appendix E: Are you an eSafe school?

Do all your staff...	Does your school...
☐ Understand e-safety issues and risks? ☐ Receive regular training and updates? ☐ Know how to escalate an issue of concern? ☐ Know how to keep data safe and secure? ☐ Know how to protect themselves online? ☐ Know how to conduct themselves professionally online? ☐ Know about the updated e-safety guidance for QTS standard Q21: Health and well-being?	☐ Have a nominated e-safety co-ordinator? ☐ Audit its e-safety measures? ☐ Have a robust AUP? ☐ Use a Becta accredited supplier for internet services? ☐ Include e-safety measures in Section 4b of your SEF? ☐ Keep an incident log and monitor your measures? ☐ Handle cyberbullying issues well? ☐ Raise awareness of the issues, e.g. through holding an assembly?
Do your learners...	**Do your parents and governors...**
☐ Understand what safe and responsible online behaviour means? ☐ Receive e-safety education at appropriate places across the curriculum? ☐ Get the opportunity to improve their digital literacy skills? ☐ Know the SMART rules? ☐ Know how to report any concerns they may have?	☐ Understand e-safety issues and risks? ☐ Understand their roles and responsibilities? ☐ Receive regular training and updates? ☐ Understand how to protect their learners in the home?

Appendix F: Website log

Request to **unblock** a website to be used by Staff and/or Learners for educational purposes.

Website Address	Reason	Staff	Date	Agreed Y/N	H/T Sig

Request to **block** a website.

Website Address	Reason	Staff	Date		H/T Sig

Appendix G: eSafety Incident Log

Date	Staff	Incident	Action

Appendix H – GLOSSARY of TERMS

The Internet and its associated services has spawned a wealth of terminology and redefined the many old words.

The Good...

- **Anti Spam** Computer program that puts into action anti-spam/spim/spit techniques
- **Anti Virus** Software Application designed to protect PCs from malicious computer code (virus)
- **AUP Acceptable Use Policy** - set of rules applied to a network, website or computer system that restricts the ways the network site or system may be used. Every school should have one!
- **CEOP** Child Exploitation and Online Protection dedicated to eradicating the sexual abuse of children. Part of UK policing tracking and bringing offenders to account. www.ceop.gov.uk Encryption The science of scrambling data be it text, audio, or video so that it can only be read by the authorised sender and recipient.
- **Cookie** A small piece of data sent from a website and stored in a user's web browser while a user is browsing a website.
- **Cloud Computing** Storing and accessing data and programs over the Internet instead of from your computer's hard drive.
- **File Sharing** A system in which users write to as well as read files or in which users are allotted some amount of space for personal files on a common server, giving access to other users as they see fit. The latter kind of file sharing is common in schools. Friend Someone on your list of contacts associated with a social networking site
- **Filtering** Software or hardware product designed to prevent access to inappropriate websites on the internet. It does this by denying or allowing access based on lists of pre-classified addresses, or by examining the web data for keywords or unwanted content.
- **Firewall** A system that prevents unauthorised access to a computer over a network, such as the internet. Firewalls can be either hardware or software businesses tend to use the former; home users the latter.
- **IM** Short for **Instant Messaging**, IM is the exchange of typed messages between computer users in real time via the Internet.
- **MMS Multimedia Messaging Service**, a system that enables mobile phones to send and receive pictures and sound clips as well as text messages.
- **Netiquette** A term referring to good behaviour while connected to the Internet. Netiquette mainly refers to behaviour while using Internet facilities such as individual Web sites, emails, newsgroups, message boards, chat rooms or Web communities.
- **OFCOM** Is the communications regulator. They regulate the TV and radio sectors, fixed line telecoms and mobiles, plus the airwaves over which wireless devices operate. www.ofcom.org.uk
- **P2P Peer-to-peer**; denoting a network or data communications in which no dedicated server is involved.
- **Patching** Software file or collection of files that fixes problems with existing applications by making changes to the program
- **Parental Control** Software Programs that can be installed on computers to limit what children – or anyone else – can do. Often used to restrict access to lists of inappropriate websites, block chatrooms and other potentially dangerous programs and even keep a

record of all email and other messages sent and received. No parental control software is completely reliable and it should only be used as part of a broader approach to online safety which involves talking to children and sharing online activities with them.

- **Password** A word or series of letters, numbers and punctuation that only you know, which you use to log on to computers, networks or online services.
- **Security Updates** New versions of programs that fix problems that have been found. Often sent out automatically, it is important that security updates are installed as soon as they are released as hackers and malware often try to make use of the errors that have been fixed.
- **SMS** Short message (or messaging) service, a system that enables mobile phone users to send and receive text messages
- **Social Network** A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services. Examples include Snapchat, Facebook, and Popjam.
- **Tweets** Tweets are text-based posts on the social networking site Twitter. They are displayed on the author's profile page and delivered to the author's subscribers known as followers. Can be restricted to a circle of friends or, by default, allow open access.
- **Webcam** A video camera designed to connect to your PC. It can be used to record video clips and still images which you can send by email, uploaded or transmitted directly over the internet for video-conferencing.

The Bad...

- **Cyber Bullying** When the Internet, mobile phones or other devices are used to send or post text or images intended to hurt or embarrass or harm another person.
- **Cyberstalking** Using information and communication technology, particularly the Internet, to harass an individual, group of individuals or organisation.
- **Digital Dirt** Approach adopted by some employers checking social network sites to see if prospective employees are drinking too much, doing drugs, trashing former employers, or letting out trade secrets on their profiles.
- **Flaming** A hostile and insulting interaction between internet users. It usually occurs in discussion boards.
- **Fraping** Concatenation of the words Facebook and rape meaning the act of changing all the details on someone's Facebook page when they leave it open and vulnerable- Personal details, relationship status, gender, sexuality, political views etc.
- **Grooming** The actions undertaken by a paedophile to befriend and establish an emotional connection with a child in order to lower the child's inhibitions in preparation for sexual abuse and/or rape. Paedophiles may initiate online conversations with potential victims to extract information about location, interests and sexual experiences.
- **Hacking** Slang term used to describe illegal access of computer systems by unauthorised users.
- **Happy Slapping** Taking and publishing pictures of assault online.
- **Identity Theft** The practice of stealing personal details (e.g. name, birth date, credit card number) and using them illegally.

- **Illegal Content** Material which is illegal under national legislation. The most common types of such content are images of sexual abuse of children, extreme sexual violence, hate and xenophobia websites.
- **Junk Mail** Unwanted email messages that are sent out to people via their email address.
- **Leeching** benefiting, usually deliberately but not necessarily illegally from others' information or effort but does not offer anything in return.
- **Malware** Malicious software that is designed to infiltrate or damage a computer system without the owner's informed consent. It includes computer viruses, worms,
- **Trojan horses**, spyware, dishonest adware and other malicious and unwanted software.
- **Pharming** The process of collecting information from a computer by hidden means - often makes use of computer programs called spyware.
- **Phishing** The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- **Sexting** The sending of explicit pictures (often self-portraits) by multimedia text message, usually via a mobile phone.
- **Spam** Unwanted email, usually of a commercial nature, sent out in bulk to an indiscriminate set of recipients.
- **Spim and Spit** Like spam but via Instant messenging (Spim) or VOIP (Spit). Spyware Malware that secretly attached to files downloaded from the internet.
- **Spyware** usually installs itself on the computer and monitors activity in order to send private information to third parties.
- **Triple XXX Content** A domain which is reserved for the online pornography industry. Also used to refer to websites which contain adult content.
- **Trojan** A computer program that takes control of the computer it is installed upon without the knowledge of the owner and is designed to access or damage sensitive data.
- **Troll** Someone who posts inflammatory, or off-topic messages in an online community, such as an online discussion forum, chat room, or blog, with the primary intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion.
- **Virus** A computer program which distributes copies of itself without permission or knowledge of the user. Viruses often hide themselves inside other programs.
- **Worm** A special type of virus that is self-replicating and can spread across many computers and harm networks, consume bandwidth and shut computers down.

Inspiring Brighter Futures

MEADOWSIDE SCHOOL WORKLOAD IMPACT ASSESSMENT 2020 APPENDIX to POLICY WRITING POLICY:

WORKLOAD IMPACT ASSESSMENT: Implementing new proposals or initiatives: Ensuring staff have capacity to take on a new task is vital to its success and their wellbeing. Our aim is to put the joy back into teaching without compromising pupil outcomes: Implement the flow chart:

Suggested Policy: e-safety

1. **Yes**

Summing Up & Judgement: Safeguarding