Medina House School
Information Communication Technology (ICT) E-Safety Policy

Our e-safety policy has been written by the school, building on the Hampshire, Isle of Wight, Portsmouth and Southampton 4LSCB E-Safety Strategy. It has been agreed by the senior management and approved by the Governors. It will be reviewed annually.

"All agencies providing services to children have a duty to understand e-safety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children"
Becta 2008- Safeguarding Children in a Digital World

What is included?

The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual. E-safety depends on the staff, governors, parents and where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies.

This e-safety policy considers the use of both the fixed and mobile internet, PC's, laptops, Ipads, digital video equipment, mobile phones, camera phones and portable media players. It will however be revised to incorporate new and emerging technologies.

Monitoring

The school will monitor the impact of this policy by:

- Logs of reported incidents (see appendix)
- Monitoring logs of internet activity (including sites visited (PREVENT – radicalisation sites, Female Genital Mutilation (FGM) , Child Sexual Exploitation (CSE) etc to further promote keeping children and adults safe in school))
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Roles and responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors: are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving termly information about e-safety incidents and monitoring reports.

The Child-Protection/Safeguarding Governor (Matt Atkins) has been appointed to the role of *E-Safety Governor* The role of the E-Safety *Governor / Director* will include:

- *Termly monitoring of e-safety incident logs*
- *Termly monitoring of filtering / change control logs*
- *reporting to relevant Governors meeting*

Headteacher:

- The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator.*

- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – in appendix.
- *The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive termly monitoring reports from the E-Safety Co-ordinator.*

E-safety coordinator

The role of the e-safety coordinator is to:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

ICT Systems Manager

is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is monitored termly in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and support staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current *school* e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the *Headteacher / Senior Leader* for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level *and* ***only carried out using official school systems***
- e-safety issues are embedded in all aspects of the curriculum and other activities

- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Child Protection / Safeguarding designated person

Will be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials – including the promotion of the PREVENT agenda – Counter Terrorism and Security Act 2015 – Prevent Duty to keep staff and children safe from radicalisation activities
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- are responsible for using the *school's* digital technology systems in accordance with the school rules.
- Will know that the use of technology to hurt or upset someone else will not be tolerated.
- will know how to report something upsetting to a trustworthy adult
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school rules also* cover their actions out of school, if related to their membership of the school

Parents

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' training, newsletters, leaflets, website / VLE and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school

Use and benefits of the Internet

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

Internet access in the school is provided via a broadband link supplied by ZEN Internet which is filtered by Surf Protect(EXA- Networks web-filtering system). EXA- Networks blocks access to any material they do not feel is appropriate. In addition to this, teachers have a responsibility to check websites before recommending them to children. The school will ensure that it meets the Prevent Duty and update legislative requirements that ensure staff and adults are kept safe whilst using the internet through the use of ZEN and filtering processes.

Benefits of using the internet in education include:

Access to world-wide educational resources.
Inclusion in government initiatives such as the Dfe's ICT in Schools
Educational and cultural exchanges between pupils world-wide;
Access to experts in many fields for pupils and staff;
Staff professional development through access to national developments,
educational materials and good curriculum practice; (whilst keeping staff and pupils safe);
Exchange of curriculum and administration data with the LA and DFE.

How will internet use enhance learning?

Where internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the person providing the lesson.
Curriculum activities that involve the use of the internet for gathering information and resources independently will help develop pupil skills in locating and evaluating material at home and in school. Subsequently this can sometimes lead to children accidently viewing a site or content they shouldn't.
As a school we have internet access that is filtered by the EXA- Networks web-filtering system, Surf Protect, which should help to avoid this. Parents may wish to consider their own monitoring programme.

How will filtering be managed?

The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved, whilst taking account of legal duties to prevent staff and children from radicalisation, FGM, CSE et.
Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate.

The use of Hector the dolphin on computers around school will ensure that if a pupil sees something upsetting they can immediately cover it and report it to a trustworthy adult who must immediately act report the site to the ICT Manager who will block the site.

If staff discover unsuitable sites, the URL (address) and content must be reported to the ICT Manager, who will be able to block the site asap through the web-based SurfProtect control panel and prevent it being accessed again.

The School will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

How will e-mail be managed ensuring safety for pupils?

Pupils may only use approved e-mail accounts on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail.
Pupils must not reveal personal details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.
Personal email or messaging between staff and pupils must not take place. .
Excessive social e-mail use can interfere with learning and may be restricted.
The forwarding of chain letters/ email is not permitted.

How should website content be managed?

The school website is maintained and kept up to date by a selected team including the ICT Manger.

The point of contact on the website must be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
Web site photographs that include pupils will be selected carefully and only when parental permission has been gained
Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
Written permission from parents or carers will be obtained from the pupils' welcome pack before photographs or media of pupils are published on the school website.
The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

The use of Social Networking and Personal Publishing sites.

The school will block/ filter access to social networking sites.
Pupils will be advised never to give out personal details of any kind which would identify them or their location.
Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary school aged pupils.

This statement relates to an employment tribunal decision:

Under normal circumstances, no members of staff must engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of the Headteacher must be sought first and appropriate professional language should always be used.

Photographic, video and audio technology

It is not appropriate to use photographic or video devices in changing rooms or toilets.
Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.

Staff may use photographic or video devices (including digital cameras, camcorders and Ipads) to support school trips and curriculum activities as long as parental permission has been sought and gained and the equipment used is school equipment not personal.

Parents should be reminded that if taking photos or videos during school productions these are only for their personal use and must not to be published on social media sights.

How can emerging ICT applications be managed?

Mobile phones will not be used during lessons or formal school time.
The sending of abusive or inappropriate text messages is forbidden.
Mobile phone cameras must not be used in school.

How will internet access be authorised?

The school will keep a record of all staff and pupils who are granted internet and email access. For members of staff this will be in the form of the "Internet and Email Acceptable Use Policies'". For all pupils, the Makaton- based "Child Friendly Policy" and the "Internet and Email Use Permission forms" are sent in the pupils' admissions letter. These records will be kept up-to-date in both a hard copy and digital format.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Isle of Wight Council can accept liability for the material accessed, or any consequences of internet access.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 amended by Police and Justice Act 2006.
Methods to identify, assess and minimise risks will be reviewed regularly and on an ongoing basis.
The Headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.
Access is strictly forbidden to any websites that involve gambling or financial scams, to sites that promote radicalisation, FGM,CSE etc.

How will the policy be introduced to pupils?

Rules for internet access will be posted in all rooms where computers are used. The rules will be presented in a child friendly format for our pupils, i.e. Makaton symbol- based.
Pupils will be informed that internet use will be monitored.
Instruction in responsible and safe use should precede internet access.
Class Teachers will explain these rules to their pupils.
A module on responsible internet use will be included in the PSHE/ICT programme covering both school and home use.
Due to the cognitive abilities and levels of understanding of the pupils at Medina House School, staff have an extra responsibility to be vigilant in order to keep the pupils in their care safe.

How will staff be consulted on e-safety and made aware of this policy?

All staff must accept the terms of the 'Internet Acceptable Use' policy before using any internet resource in school.
All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School ICT Policy and E-safety policy and have its importance explained.
The monitoring of internet use is a sensitive matter. Staff who monitor internet use procedures will be supervised by senior management.
Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
Staff will be provided with training and kept up-to-date on e-safety issues.
Schemes of work will be in place for staff to teach and make their pupils aware of how to keep safe when using the internet.

How will the ICT system security be maintained?

The school ICT systems will be reviewed regularly and on an ongoing basis with regard to security.
Virus protection will be installed and updated regularly.
School laptops used outside of school will be encrypted.
Personal data sent over the internet will be encrypted or otherwise secured.
Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
Files held on the school's network will be regularly checked.
The IT Manger will ensure that the system has the capacity to take increased traffic caused by internet use.

How will parents' support be enlisted?

Parents' attention will be drawn to the School Internet Policy and E-safety policy in newsletters, the school brochure and on the school website.

E safety training will be provided yearly to parents. Leaflets will be made available to keep their children safe when using technology outside of school.

Other related policies: Child Protection, Social Networking, Anti-Bullying , Whistle Blowing, Electronic Mail – Acceptable Use Policy, Internet – Acceptable Use Policy

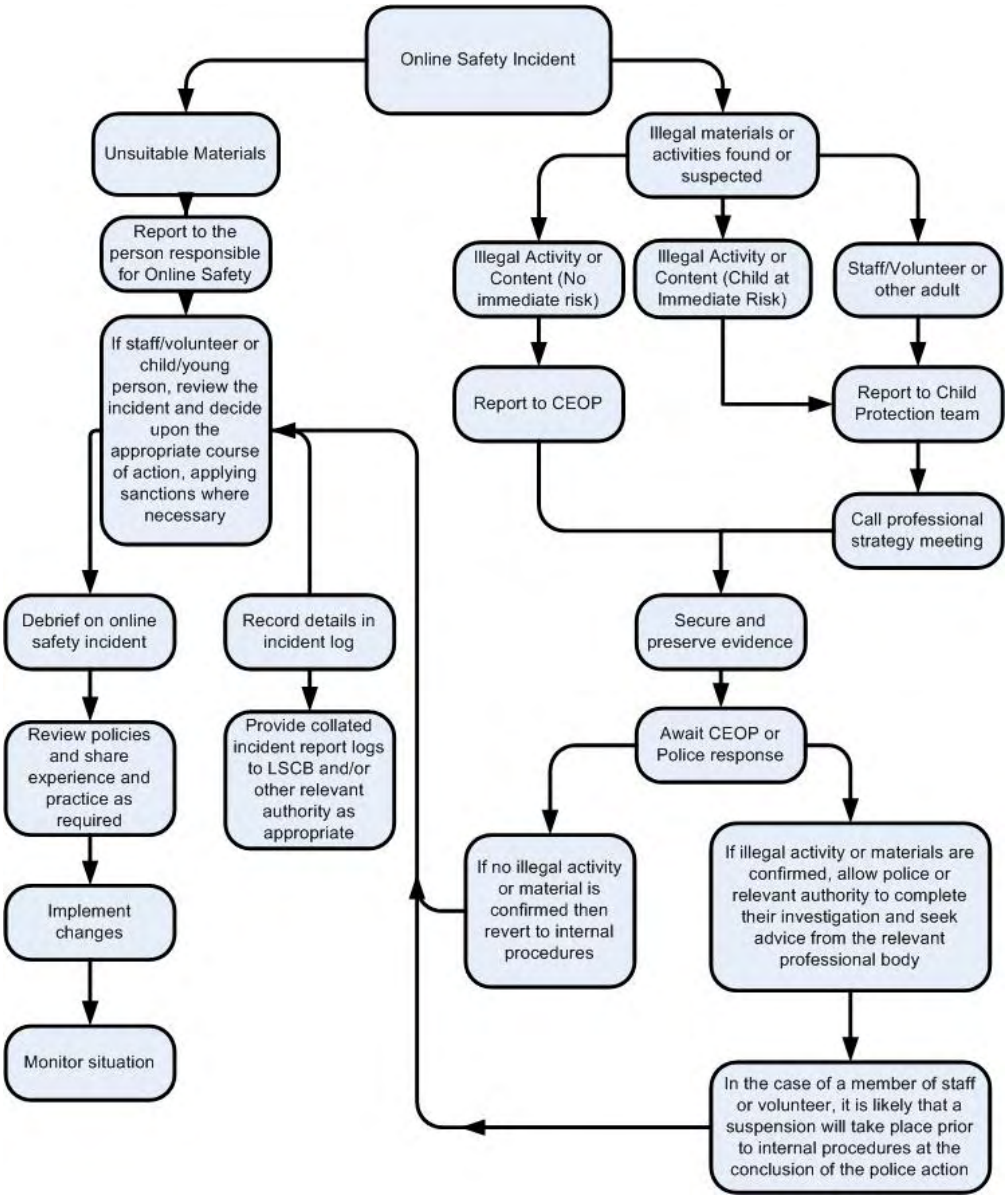
Date Agreed : …….

Signed:……
Chair of Governors

To be reviewed: November 2018

APPENDIX

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school / academy network by sharing username and passwords									
Attempting to access or accessing the school / academy network, using another student's / pupil's account									
Attempting to access or accessing the school / academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's / academy's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data eg holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy								
Using proxy sites or other means to subvert the school's / academy's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								