St Mary's CE Primary eSafety & Data Security Policy September 2019

1 Corinthians 16:14

Reviewed May 2019

Presented to Governors: ……

St Mary's Church of England Primary School is a warm, friendly and welcoming Church school that provides high quality education for all its pupils. As a Church school we hold our Christian values at the heart of everything we do. These are: Love; Respect; Determination; Courage; Compassion; and Honesty.

It is very important to us that the children are happy and experience the best education possible. We value strong links and a close partnership between home, church and school and recognise the importance of trust and shared responsibility in education

E- Safety Policy for ICT Acceptable Use

The member of school staff responsible for e-safety is Simon Owen.

They are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the college community. He may also be required to deliver workshops for parents.

Internet use and Acceptable Use Policies (AUPs)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role.

The Acceptable Use Policies used can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip.

This can be found in appendix 2

AUP's will be reviewed annually. All AUPs will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise.

Staff should always use a school camera to capture images and should not use their personal devices. Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
Photos taken by the school are subject to the Data Protection Act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

St Mary's CE Primary School recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.

The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

St Marys CE Primary School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in the classrooms, toilets, changing rooms or in the play areas at any time. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. If staff need to make an emergency call, they must do so either in the main or Headteacher's office. Staff must ensure that there is no inappropriate or illegal content on the device.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the nursery/school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Members of staff may only contact a parent/carer on school approved mobile phones. Pupils should not use mobile phones within the school grounds and should not bring in a mobile to school at any time.

The school is not responsible for the loss, damage or theft of any personal mobile device

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises. If they wish to make or take an emergency call they may use either the main or the manager's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard

children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers/practitioners or volunteers at the school understand the difference between appropriate and inappropriate sharing of images.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails

Staff and pupils should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Staff and pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Managing e-Mail

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the ICT subject leader or headteacher) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT National Curriculum.
- However you access your e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending Emails

- Use your own school e-mail account so that you are clearly identified as the originator of a message.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

Check your e-mail regularly

- Never open attachments from an untrusted source

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of e-mails is not allowed

Security and passwords

It is the responsibility of each member of staff to keep their passwords secure. Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').
All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to be used in school.

School administrative systems are accessed via VDI and are managed and backed up through service level agreement with HBC ICT services.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported.
Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the senior leadership team in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. trusted adult, ChildLine).

Complaints

Complaints and/ or issues relating to eSafety should be made to the subject leader or Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the subject leader or the headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the headteacher, depending on the seriousness of the offence; investigation by the Headteacher/ LA immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

eSafety

eSafety - Roles and Responsibilities

As eSafety 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 eSafety co-ordinator in this school is the headteacher. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance.

Senior Management and governors are updated by the Headteacher 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 school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

E-Safety Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

- A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- Regularly auditing, review and revision of the computing curriculum
- E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
- Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc.

Additionally,

- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour
- Pupils are taught to acknowledge copyright and intellectual property rights in all their work.
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Staff

- A planned programme of formal e-safety training is made available to all staff. Additionally, all staff have CPD on the Prevent duty.
- E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
- All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
- Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate
- The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
- The school takes every opportunity to research and understand good practice that is taking place in other schools
- Governors are offered the opportunity to undertake training.

Parents and the wider community

There is a planned programme of e-safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety co-ordinator with input from the e-safety committee.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

Staff will preview any recommended sites before use.

Raw image searches are always supervised by staff.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources

Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.

On-line gambling or gaming is not allowed.

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Managing Other Web Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavors to deny access to social networking.

All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

Our pupils are asked to report any incidents of Cyberbullying to the school.

Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher
Schools in England (and Wales) are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

St Mary’s CE Primary ensure that children are safe from terrorist and extremist material when accessing the internet in school. As with other online risks of harm, every teacher is aware of the risks posed by the online activity of extremist and terrorist groups. All staff undergoes Prevent training. Halton Borough Council provides St Mary’s with web filtering to keep our children safe.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

Ensure that any school information accessed from your own PC or removable media equipment is kept secure.

Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

Ensure the security of any personal, sensitive, confidential and classified information

contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

Only download personal data from systems if expressly authorised to do so by your manager.

You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses.

Never interfere with any anti-virus software installed on school ICT equipment that you use. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Security

The school gives some staff access to the school website and Shared Drive with a unique username and password

It is the responsibility of everyone to keep passwords secure

Staff are aware of their responsibility when accessing school data

Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

As a user of the school ICT equipment, you are responsible for your activity.

Ensure that all ICT equipment that you use is kept physically secure.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
It is imperative that you save your data on a frequent basis to the school's share drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network.

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

The installation of any applications or software packages must be authorised by the Headteacher, fully licensed and only carried out by your ICT support

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency or via Halton Borough Council. This should 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 over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We 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
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

St Mary's CE Primary School

Pupil Acceptable Use Agreement / eSafety Rules

These rules will keep me safe, keep my information private, and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will not attempt to read any personal information on paper or in a computer file unless that information is meant for me.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not attempt to learn logins and passwords that belong to other people.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I will respect this.
- I will not attempt to visit internet sites that I know the school has banned.
- I will only e-mail the people I know, or those a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will maintain my data and personal security: I will not give my home address, phone number, send a photograph or video, give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.
- I will not bring a mobile phone into school except in exceptional circumstances and when specifically allowed by the Headteacher. If I bring in a mobile phone to school, I will ensure that is given to the Headteacher or my class teacher to be securely locked away until the end of the day.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

I have read and understood these rules and agree to them.

Signed: …….…… Date ……..……

Do everything in love

1 Corinthians 16:14

Learning to Love, Loving to Learn

St Mary's School

St. Marys Church of England Primary School
Castlefields Avenue South
Halton Runcorn
Cheshire WA7 2NR
Tel: 01928 565995
Fax 01928 569298
e-mail head.stmarys@halton.gov.uk
Website www.stmaryshalton.co.uk

Head Teacher Rachel Tainsh B.A. (Hons) P.G.C.E

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies have become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the completed slip at the bottom of this page along with your child's signature on the Acceptable use Agreement to say that they have read and understood the safety rules.

If you have any concerns or would like some explanation please contact us.

Simon Owen
ICT Subject Leader

St Mary's CE Primary School

We have discussed this and …….....(child name) agrees to follow the eSafety rules and to support the safe use of ICT at St Mary's CE Primary School.

Parent/ Carer Signature ……

Class …… Date ……

St Mary's CE Primary School

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher or the ICT Subject Leader.

- I will only use the approved school's email accounts/ Internet / Website (Learning Platform) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will ensure that personal data (such as data held on SIMs or CPOMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission of the Subject Leader.
- Images of pupils and/ or staff will only be taken on school cameras, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I will report unsuitable content and/or ICT misuse to the e-safety officer.
- I will set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- I will respect copyright and intellectual property rights.

I know that anything I share online may be monitored. I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - inappropriate images
    - promoting discrimination of any kind
    - promoting violence or bullying
    - promoting racial or religious hatred
    - promoting illegal acts
    - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature ……..…… Date ……..……

Full Name ……..(printed)

Job title ……..

SUPPORTING DOCUMENTS

This policy, is linked to the following school policies:

- Keeping Children Safe in Education; Statutory guidance for schools
- and colleges (2019)
- Working Together to Safeguard Children (2018)
- Prevent Duty Guidance (HM Government 2015)
- Prevent Strategy (HM Government 2011)
- What to do if you're worried a child is being abused (2015)
- Information Sharing (DfE: 2015)
- Safeguarding and Child Protection Policy
- Health and Safety Policy
- Home School Agreement
- Behaviour Policy
- Anti-bullying Policy
- PSHCE Policy
- Staff Code of Conduct
- Freedom of Information Policy