St Mary's Catholic Primary School

Living and Learning Together – Shining in our Faith

Online Safety Policy 2025-2026

(Reviewed and approved by Curriculum Committee – September 2025
To be reviewed: September 2026)

Statement of Intent

St Mary's Catholic Primary 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 four areas of risk:

•**Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

•**Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

• **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

• **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams. The measures implemented to protect pupils and staff revolve around these areas of risk.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

This policy applies to all members of the St Mary's Catholic Primary School community including staff, pupils, volunteers, parents, carers, and visitors who have access to, and are users of, school digital technology systems at St Mary's Catholic Primary School.

Our Online Safety Policy has been written by the school, building on Government guidance. It has been agreed by the staff and approved by governors.

Roles and Responsibilities

The governors will be responsible for:

Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

• Ensuring the DSL's remit covers online safety.

• Reviewing this policy on an annual basis.

• Ensuring their own knowledge of online safety issues is up-to-date.

• Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

• Ensuring that there are appropriate filtering and monitoring systems in place.

• Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

• Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

• Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them

The Headteacher will be responsible for:

Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

• Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

• Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.

• Ensuring online safety practices are audited and evaluated.

• Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

• Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.

• Working with the DSL and governing board to update this policy on an annual basis.

The Online Safety Lead/DSL will be responsible for:

• Taking the lead responsibility for online safety in the school.

• Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

• Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.

• Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

• Ensuring safeguarding is considered in the school's approach to remote learning.

• Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.

• Understanding the filtering and monitoring processes in place at the school.

• Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

• Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

• Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

• Reporting to the governing board about online safety on a termly basis.

• Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.

• Working with the headteacher and governing board to update this policy on an annual basis.

Digital devices and technology

Smart Watches:

Must not be worn by children.

Staff must not use these for any other purpose than to utilise basic watch functions during contact with children.

Mobile Phones:

Children:

• Are forbidden from having mobile phones on their person whilst on school premises.

• Must hand their mobile phones to the school office upon arrival at school and it is their responsibility to retrieve them at the end of the school day.

• Must switch their phone off and only switch it on again when they have left the school grounds.

Staff:

• Personal mobile phones belonging to members of staff must be switched off for the duration of the school day unless they are being used in the Staffroom or Office areas.

• Staff are permitted to use their mobile phones where pupils are not present (Staffroom, Office areas, classroom at play/lunchtimes). Outside of this, they should only be used at the staff members' discretion (To contact if an emergency for example).

• Staff must not access their mobile phone when children are present in the room.

• No images, video or audio of children is to be recorded on personal mobile phones without explicit permission being given by the head teacher.

Use of digital media (I pads, cameras and recording devices):

Staff:

• The school has access to and use of a range of digital cameras and tablets. The cameras and the memory cards within them are forbidden from being taken off the premises by any member of staff unless explicit permission is given by the head teacher or the adult is a designated person.

• Tablets come under the same restrictions as the digital cameras.

• Written permission is obtained from parents for photographs of their children to be taken and used. New arrivals are presented with the same permission form.

• Staff are given a list at the start of the academic year of children whose parents have not given permission for their photographs to be used on the school website, social media, newspaper articles or publically visible displays.

• All staff members employed by the school have permission to take images/video/audio of the children in school but not on personal recording equipment as stated in the Mobile phone usage section of this document.

Parents:

• Parents are permitted to take photographs of their own children on school premises on the provision that the photographs are for their own use.

• Parents are aware that taking a photograph that includes other children could constitute a potential breach of Data Protection legislation.

• If parents want to take a photograph/video that includes other children then they need to obtain permission from the parents of the other children.

• Parents are aware that uploading images/video of their child alongside other children to social network sites is not acceptable unless specific permission has been obtained from the parents of the other children.

Storage of photographs/video:

• Any storage of photographs/video or audio of children or staff on school devices is to occur on the school server.

• No photographs/video or audio of children is to be stored on removable USB drives unless the drives are being kept securely on school premises.

• Staff are not to remove school cameras or tablets containing photographs/video or audio of children from the school premises except for designated persons for designated purposes.

• Once children's images have been used for display they need to be disposed of by shredding.

• In the event of a third party taking photographs of the children e.g. newspaper, written permission should be obtained from the parents of the children informing them of the way in which their child's image will be used.

E-mail:

• All staff have access to Outlook system for work-based e-mail.

• Staff are permitted to access their personal e-mail accounts on school premises on personal devices at playtimes, lunchtimes or at other times when no children are present.

• Only official e-mail accounts or password protected staff-designated e-mail accounts are to be used for professional communication. Staff are to only open links or documents that they know are genuine.

• Any incidents of SPAM on official e-mail accounts should be reported to the Online Safety Lead.

• All e-mails must be sent with the e-mail disclaimer at the bottom.

Social Networks:

Staff:

• Staff are permitted to have social network accounts (Facebook, Twitter, Pinterest etc.) but it is not acceptable to post content that: brings the school into disrepute; leads to valid parental complaints; is deemed as derogatory towards the school and/or its employees; is deemed as derogatory towards pupils, parents or carers; brings into question their appropriateness to work with children and young people.

• All staff social media accounts must be private and not open to public scrutiny. If staff are unsure as to whether their social media is private they should consult with the Online Safety Lead.

• It is not acceptable for staff to accept friend/follower requests from students who are currently enrolled at the school unless they are family members.

• Communication with past pupils, parents or siblings of pupils (not enrolled at school) is strongly discouraged particularly if the pupils are under the age of 18 years of age.

• In the case of incidents on social media (outside of school hours) affecting children's behaviour or causing issues during school hours then a meeting will be arranged with the DSL or deputy DSL, Online Safety Lead, the child who has committed the incident and the child's parents to deal with the "spill over" into school hours.

Parents:

• Parents should be aware that posting inappropriate comments about individual members of staff or children can be construed as online bullying. If this situation arises then the parent(s) in question will be invited into school to discuss their issues and asked to remove the offending post.

• It is not acceptable for parents to discuss issues that they may be experiencing at school on social media as it may bring the school into disrepute. It is preferred that the parents in question make an appointment with the relevant staff member so that their issue can be dealt with directly and then the offending post deleted.

• As stated previously; parents are aware that uploading images/video of their child alongside other children to social network sites is not acceptable unless specific permission has been obtained from the parents of the other children.

• Parents are aware that the legal age requirement for children to have social media profiles and instant messaging service apps, is 13 years of age. If they choose to allow their child to have a social media profile under this age then they are causing the social media network in question to break the law.

Managing Online safety

Preventing Extremism

The school is aware that it has a role to play to prevent radicalisation and extremism. To prevent the radicalisation of young people the school:

• Has a filtering system to block out inappropriate websites.

• A reporting system in place for both staff and pupils to keep a record of any incidents which occur.

• Has received training on awareness and prevention of extremism. (PREVENT)

• Has AUPs in place for staff, parents and children.

• Through Online Safety, teaches the children to become critical learner and so they know what is acceptable or unacceptable even though filters are in place School Website

• The Headteacher and Bursar are responsible for the school website.

• They are aware of the information that should be included on the school website according to the School Information Regulations.

• It is the designated persons' responsibility to ensure the information on the school website is kept up-to-date.

• Downloadable materials are to be made accessible in pdf format only, to prevent the content being manipulated and redistributed without school's knowledge or consent.

Infrastructure & Technology

In order to keep children safe, the school subscribes to the Lancashire Grid for Learning so internet filtering (BT netsweeper) is provided by default and it is installed and configured on all devices.

Access

• When accessing school equipment and online materials children are supervised by a trusted adult and protected by the online filtering system.

• Class accounts for the server restrict their access to certain areas of the network.

• Access to confidential data is restricted to the school office e.g. SIMS etc.

• Staff members have access to all school systems as required.

• All users of the school network have a secure username and password.

• The administrator password for the school network is available to the school technician.

Managing the network and technical support

• All servers, wireless systems and cabling are securely located and access is restricted.

• Critical updates and software installation involving executable files is completed by the school technician who visits every three weeks.

• Security breaches should be reported to the Online Safety Lead or Headteacher.

Dealing with incidents / Illegal offences:

• Any suspected illegal material or activity must be reported to the head teacher immediately who must refer this to the relevant external authority.

• Illegal content must be reported to the Internet Watch Foundation who have a licence to investigate, schools do not.

• Details of what constitutes illegal offences can be found at http://iwf.org.uk Inappropriate use (a copy to be provided to each classroom.

INAPPROPRIATE USE: INCIDENT PROCEDURE AND SANCTION

Incident	Procedure & Sanction
Accidental access to inappropriate materials	• Minimise the webpage/turn off the monitor. • Inform Online Safety Lead • Enter the details in the incident log and report to LGfl filtering services if necessary Using other people's logins and passwords maliciously
Using other people's logins and passwords maliciously.	• Inform the Online Safety Lead • Enter the details in the incident log • Additional awareness raising Online Safety issues and the A.U.P. with individual child/class • More serious or persistent offences may result in further disciplinary action in line with the Behaviour Policy • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	Inform the Online Safety Lead • Enter the details in the incident log • Additional awareness raising Online Safety issues and the A.U.P. with individual child/class • More serious or persistent offences may result in further disciplinary action in line with the Behaviour Policy • Consider parent/carer involvement.
Bringing inappropriate electronic files from home.	Inform the Online Safety Lead • Enter the details in the incident log • Additional awareness raising Online Safety issues and the A.U.P. with individual child/class • More serious or persistent offences may result in further disciplinary action in line with the Behaviour Policy • Consider parent/carer involvement.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems.

All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE
- Computing

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

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.

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

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy. If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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 (regularly updated parental controls information is available in school and on the website.)

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

• Parents' evenings

•Online safety specific monthly newsletters and resources

• Online resources

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2025. Any changes made to this policy are communicated to all members of the school.

The team responsible for dealing with Online Safety incidents is (any combination of):

- The Online Safety Lead
- Computing lead
- DSL and Back up DSL
- Designated Online Safeguarding Governor
- Head Teacher

The Online Safety Policy will be reviewed annually.

APPENDICES:

Appendix 1: Acceptable Use Policy for children

Appendix 2: letter to parents/carers to explain A.U.P.

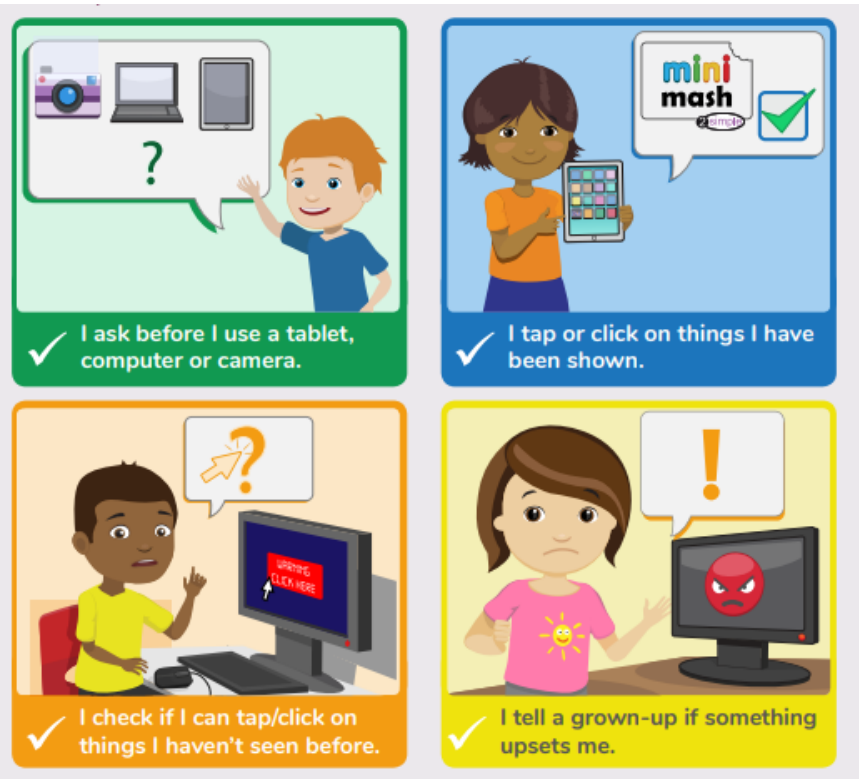
Appendix 3: Acceptable Use Policy for staff

St Mary's Catholic Primary School

Living and Learning Together – Shining in our Faith

Acceptable use policy for Nursery and Reception Class

September 2025



My Name: _____ Class: _____

Parent/ Carer Signed: _____ Date: _____

St Mary's  **Catholic Primary School**

Living and Learning Together ***– Shining in our Faith***

Acceptable use policy for Key Stage 1

September 2025

- ✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ✓ I only open activities that an adult has told or allowed me to use.
- ✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ✓ I keep my passwords safe and will never use someone else's.
- ✓ I know personal information such as my address and birthday should never be shared online.
- ✓ I know I must never communicate with strangers online.
- ✓ I am always polite when I post to our blogs, use our email and other communication tools.

My Name: _____ Class: _____

Parent/ Carer Signed: _____ Date: _____

St Mary's Catholic Primary School

Living and Learning Together – Shining in our Faith

Acceptable use policy for Key Stage 2

September 2025

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ✓ I will keep my username and password secure; this includes not sharing it with others.
- ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ✓ I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- ✓ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- ✓ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- ✓ Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = is it true?
  H = is it helpful?
  I = is it inspiring?
  N = is it necessary?
  K = is it kind?

- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

My Name: _____ Class: _____

Parent/ Carer Signed: _____ Date: _____

St Mary's Catholic Primary School

Living and Learning Together – Shining in our Faith

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites and Instant Messaging Services that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School Online Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing Online Safety as part of your child's learning, we will share with you monthly "Online Safety newsletter" which can be found on the school website Online Safety | St Mary's Catholic Primary School (stmaryscps.co.uk). If you would like to find out more about Online Safety for parents and carers, please visit the Lancsngfl Online Safety website http://www.lancsngfl.ac.uk/Online Safety. If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Mrs Dawn McGrath.

Yours sincerely,

Mrs Joanne Preston

Headteacher

St Mary's Catholic Primary School

Living and Learning Together – Shining in our Faith

Staff (and Volunteer) Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

• That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the school digital technology and communications systems.

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

• I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. • I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

• I will only use my personal mobile phone in the staff room, office or classroom when no children are present.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.

Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only use social networking sites in school in accordance with the school's policies.

• I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

• I will not engage in any on-line activity that may compromise my professional responsibilities. The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

• When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not disable or cause any damage to school equipment, or the equipment belonging to others.

• I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.