Enjoy, Learn, Succeed

OfSTED Unique Reference Number (URN): 113264

Intent Drivers – Our Core Values			
Perseverance	Aspiration	Respect	Collaboration

www.marytavyandbrentorprimary.co.uk

Online-Safety Policy

Policy Version	January 2020
Approved/reviewed by Governors annually	January 2023
Review date annually	January 2024

Mary Tavy and Brentor Community Primary School

Online-safety policy 2023

Rationale

At MTB we believe that online (E-Safety) is an essential element of safeguarding our children and adults in the digital world we live in. We identify that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
We have a duty to provide our school community with quality Internet access. We identify there is a clear duty to ensure that children are protected from potential harm online.

Contents

1. Introduction and Overview

The purpose of this policy is to:

- Clearly identify key principles expected of all members of the school community at MTB Primary School with regards to the safe and responsible use of computing based technology to ensure MTB is a safe and secure environment.
- Safeguard and protect all members of our MTB Primary School Community online and comply with GDPR (General Data Protection Regulation).
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet.
- Have clear procedures to use when responding to online safety concerns cross
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The main areas of risk for our school community can be summarised as follows:

Content

- ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases)
- exposure to inappropriate content, including online pornography,

Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.

- Data breach
- hate sites, sites inciting radicalisation and/or extremism
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords
-

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Inappropriate Message

This policy applies to all members of Mary Tavy and Brentor Community Primary School (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of MTB Primary School COMPUTING systems , both in and out of MTB Primary School.
The Education and Inspections Act 2006 empowers Head teacher to such extent as is reasonable, to regulate the behavior of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
MTB Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online-safety behaviour that take place out of scho

Role	Key Responsibilities
Head teacher Clare Davies	• To take overall responsibility for Online-safety provision • To take overall responsibility for data and data security GDPR compliant • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g SWGFL • To be responsible for ensuring that staff receive suitable training to carry out their Online-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious Online-Safety incident. • To receive regular monitoring reports about Online-safety from Computing Coordinator • To ensure that there is a system in place to monitor and support staff who carry out internal Online-safety procedures
Online-safety Computing Co-ordinator / Designated Child Protection Leader Kere Ascot	• takes day to day responsibility for Online-safety issues and has a leading role in establishing and reviewing the school Online-safety policies / documents • promotes an awareness and commitment to Online-safeguarding throughout the school community • ensures that Online-safety education is embedded across the curriculum • liaises with school COMPUTING technical staff • To communicate regularly with SLT and the designated Online-safety Governor discusses current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online-safety incident • To ensure that an Online-safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in Online-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • Regulate sharing of personal data • restrict access to illegal / inappropriate materials • restrict inappropriate on-line contact with adults / strangers • restrict potential or actual incidents of grooming • restrict cyber-bullying and use of social media • To oversee the delivery of the Online-safety element of the Computing curriculum • To address Online-safety issues as they arise promptly
Governors	• To ensure that the school follows all current Online-safety advice to keep the children and staff safe • To approve the Online-safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about Online-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online-safety Governor To support the school in encouraging parents and the wider community to become engaged in Online-safety activities

Role	Key Responsibilities
Parents/carers	• To support the school in promoting Online-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images To read, understand and promote the school Pupil Acceptable Use Agreement with their children
Network Manager/ technician The school uses third party company – TME Computing Curriculum Leader	• To report any Online-safety related issues that arises, to the Computing Co-ordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school Computing system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • SWGFL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's Online-safety policy and technical information in order to effectively carry out their Online-safety role and to inform and update others as relevant • that the use of the *network / remote access / email/School Facebook account* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Online-safety Co-ordinator/GDPR officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's Online-security and technical procedures
GDPR Officer	• To take overall responsibility for data and data security • To ensure that all data held on pupils on the school office machines have appropriate access controls in place
SWGFL Nominated contact(s)	• To ensure all SWGFL services are managed on behalf of the school including maintaining the SWGFL USO database of access accounts
Teachers	• To embed Online-safety issues in all aspects of the curriculum and other school activities. To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To embed Online-safety issues in all aspects of the curriculum and other school activities

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's Online-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of Online-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Online-safety coordinator • To maintain an awareness of current Online-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good Online-safety practice when using digital technologies out of school and realise that the school's E- Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the creation/ review of Online-safety policies
Parent Support Computing Coordinator	• Educating Parents and raising awareness as instructed by Computing Coordinator

Role	Key Responsibilities
Parents/ carers	• To access the school website/ online platform account accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school • To seek parental consent if the external party intends to use pupil photograph

Communication:

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure Online-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
- interview/counselling by teacher/ Online-safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to LA / Police.

- Our Headteacher acts as first point of contact for any Online-safety complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti- Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures

Review and Monitoring

The Online-safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an Online-safety coordinator who will be responsible for document ownership, review and updates.
- The Online-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online-safety policy has been written by the school Online-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum -Pupil Online-safety curriculum

Our school

- Has a clear, progressive Online-safety education programme as part of the Computing curriculum / RHSE curriculum. It is built on national guidance and Purple Mash computing scheme of work. This covers a range of skills and behaviours appropriate to their age and experience, including:

to STOP and THINK before they CLICK

- to develop a range of strategies to evaluate and verify information before accepting its accuracy.
- to be aware that the author of a web site / page may have a bias or purpose and to develop skills to recognise what that may be.
- to know how to narrow down or refine a search.
- to ensure children know how to access online platforms safely and are aware that they should not share their log in details with anyone (see AUAs).
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- to understand acceptable behaviour when using an online environment, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post photos or videos of others without their permission.

- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign/will be displayed throughout the school.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop- ups; buying on-line; on-line gaming / gambling;

Staff and governor training

Our school

- Ensures staff and governors have had GDPR training and know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on Online-safety issues, GDPR and the school's online-safety education program; Termly updates in staff meetings.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online-Safeguarding policy and the school's Acceptable Use Policies.

- **Parent awareness and training**

- Our school runs a rolling programme of advice, guidance and training for parents to ensure that principles of Online-safety behaviour are made clear, including:
- Information leaflets; in school newsletters; on the school web site Facebook
- demonstrations, workshops, practical sessions held at school;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In our school, all users:

- are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at EYFS it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good Online-safety practice when using digital technologies out of school and realise that the school's Online-safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's Online-safety policy and using the school COMPUTING systems accordingly, including the use of mobile phones, and hand held devices.
- Are responsible for pupil data safe so that it is GDPR compliant

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

- the school does not permit parents/carers to take photographs and videos of other children at school events and are reminded that they are only for personal use and that the school requests that photos/videos are not shared on any social networking site such as Facebook, WhatsApp, snapchat, twitter etc.

Incident Management

In Our school:

- there is strict monitoring and application of the Online-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with Online-safety issues.
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in Online-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- parents / carers are specifically informed of Online-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Data breaches are reported to our GDPR officer Mrs R Hillier and if need it be then to Information Commissioners Office (ICO)
  Any safeguarding incidents are reported Designated Safeguarding Leads (DSL) Mrs Davies or to Mrs K Ascot/Mrs R Hillier (Deputy Safeguarding Leads)
- all the Online-safety incidents are reported to the Head of School/Computing coordinator.
- the Head teacher Computing Coordinator/Class Teacher keeps the records of the Online-safety incidents.

4. Managing the Computing infrastructure

Internet access, security (virus protection) and filtering

Our school:
Has the educational filtered secure broadband connectivity through the
SWGFL and so connects to the 'private' National Education Network;

- Uses the SWGFL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature
, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from SWGFL) etc and network set-up so staff and pupils cannot download executable files;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the SWGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment.
- Requires staff to preview websites before use [where not previously viewed or cached] Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; https://swiggle.org.uk yahoo for kids or ask for kids , Google Safe Search
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the [*/ teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or SWGFL Helpdesk, as necessary.
- Makes clear all users know and understand what the 'rules of appropriate use' are, GDPR compliance and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- Computing devices provided by school to members of staff are regularly checked by the IT technicians.

- **Network management (user access, backup)**
  Our school
- Uses Technicians employed by TME
- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Ensures the Systems Administrator / network manager is up-to-date with SWGfL services and policies / requires the Technical Support Provider to be up-to- date with SWGfL services and policies;
- Storage of all data within the school will conform to the GDPR requirements
- Staff will only use OneDrive/teams folders or external hard-drive to hold any data about pupils

To ensure the network is used safely, Our school:

- Ensures staff read and sign that they have understood the school's Online-safety Policy, Data Protection Policy, Data Retention Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. Guest users do not have access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with own unique network log-in username and password.
- All pupils have their own unique username and password which gives them access online platforms (Purple Mash, Office)
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day unless there is a clear reason for leaving the machine on.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via Office 356
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children,
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school computer systems regularly with regard to health and safety and security.

Passwords policy

- Our school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords to enter our MIS systems
- We require staff to change their passwords into the MIS, SWGfL USO admin site, regularly.

E-mail

- All staff to adhere to school's Email protocol and email use policy
- Provides staff with an email account for their professional use, Office 365 and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use their personal school email account.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Any apps educational (mathletics, TTR Spelling Shed, spag.com) and /or Classroom management (Purple Mash) used by school are GDPR compliant.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary, to the Police.
- Any personal or business use for illegal, threatening, offensive, obscene, pornographic or libellous purposes by staff is strictly prohibited.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of SWGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these,SWGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- Pupils are introduced to and use e-mail as part of the Computing scheme of work. They can only use email through Purple Mash platform and cannot email external people.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
- not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise.
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.
- that they should think carefully before sending any attachments.
- embedding adverts is not allowed.
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
- not to respond to malicious or threatening messages.
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
- that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e- safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use office 365 systems for professional purposes
- Access in school to external personal e mail accounts is not permitted and may be blocked
- Never use personal email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- the sending of multiple or large attachments should be limited and may also be restricted by the provider of the service being used.
- the sending of chain letters is not permitted.
- embedding adverts is not allowed.

- All staff sign our school Agreement Form AUP to say they have read and understood the Online-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
- A letter sent to anyone using the school letterhead must be approved by the head teacher.
- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of school events on personal social networking sites such as Facebook. Twitter etc
- Staff must not use social networking sites within lesson times
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, admin@marytavyandbrentor.devon.sch.uk
- photographs published on the web do not have attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geo-data in respect of stored images
- We expect teachers using' school approved blogs to password protect them and run from the school Purple mash platform.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open their own spaces to their students.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils' parents/ carers or school staff
- Data about pupil/ staff or parents is not shared on social media
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing Our school

- Only uses google classroom meet for video conferencing, (pupils and staff to use their **school google log in** details)
- Where communication is with children and teachers it should never be 1:1 there should always be a parent in attendance and, a second member of staff.

5. Data security: Management Information System access and Data transfer (Also check our Data Protection Policy, Data Retention Policy and safeguarding policy)

Strategic and operational practices

At Our school:

- Staff to report any incidents where data may have been breached to the GDPR officer Mrs R Hillier
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure All staff are DBS checked and records are held in one central record in the school office.

- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system, so we know who has signed.
  - staff,
  - governors,
  - pupils
  - parents
- This makes clear staffs' responsibilities regarding data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect, and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platforms access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be

Technical Solutions

- We require staff to log-out of systems when leaving their computer.
- We use the DfE S2S site to securely transfer CTF pupil data files to other
- We use the Devon County Council admissions area (based on USO FX) to transfer admissions data.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are managed by TME staff.
- We use in house secure back-up for disaster recovery on our network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
  - Portable equipment loaned by the school (for use by staff/pupils at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using crosscut shredder.

6. Equipment and Digital Content

School Mobile Devices such as Ipads, and laptops are used on the school network.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, students & parents' or

visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

- Parents/carers/visitors are not permitted to use their mobile phones/take pictures and/or videos of staff and/or pupils in the school playground.
- Student mobile phones, MP3 players, iPads, smart watches which are brought into school must be turned off (not placed on silent) and handed in to the Office staff on arrival at school. They must remain turned off and locked away until the end of the day.
- All visitors are requested to tun off their mobile phones.
- Recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Staff may use their phones during break times in the office or staff room. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times.
- Staff mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should always be switched off or silent.
- Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- The Bluetooth or similar function of a mobile phone should always be switched off and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally owned mobile devices without the prior consent of the head teacher.
- Images and content recorded for twitter updates will be deleted from the school equipment once it is posted.

- ***Students' use of personal devices***
- The School strongly advises that student mobile phones/smart watches/tablets/MP3 players should not be brought into school. The school takes no responsibility for loss or damage of any personal devices brought to school.
- The School accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Student mobile phones/smart watches/tablets/MP3 players should be handed to the office upon arrival. Students found in possession of a mobile phone and or smart watch during an exam will be reported to the appropriate examining body. This

- may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences. However, in case if a student has sent an inappropriate message or photo to another student at any time and the matter is brought to the attention of the school then the device will be confiscated and returned at the end of the academic year. Parents/carers will be immediately informed.
- Students will be provided with school IPads/cameras/notebooks/laptops to use in specific learning activities under the supervision of a member of staff. Such devices will be set up so that only those features required for the activity will be enabled.
- No students should use his or her mobile phone or personally owned device in school. Any personal devices used in school by a pupil will be confiscated.

- ***Staff use of personal devices***
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families outside of the setting in a professional capacity unless on a school trip.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and
- mobile phones or personally owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- The only circumstance in which a teacher can take a picture on the mobile phone is so that the image can be uploaded on the school 's official Facebook / Instagram accounts. It should only be done with prior consent from the Head teacher. The image should be taken in presence of teacher. The image/images should be deleted immediately once it is uploaded on the school's official Facebook/ Instagram account.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting parents, then they should hide their caller identification. They can do so by inputting 141 to hide their own mobile number for confidentiality purposes.

Digital images and video In Our school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Photos/videos taken on school iPads are stored on the school network.
- Pupils are taught about how images can be manipulated in their Online-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their COMPUTING scheme of work;
- Pupils are advised to be incredibly careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

Online-safety Audit

The self-audit in should be completed by the member of the Management Team responsible for the Online-safety policy.

Is there a school online-safety Policy that complies with SWGFL guidance?	Yes
Date of latest update (at least annual): September 2021	
The Leadership team member responsible for online-safety is:	
The governor responsible for Online-Safety is:	Tim Collingwood
The designated member of staff for child protection is;	Clare Davies
The online-Safety Coordinator is:	Kere Ascot
The online-Safety Policy was approved by the Governors on	
The policy is available for staff :	In the staff room
The policy is available for parents/carers at:	On the website