St Mary's C of E School
Truro

Computing and
E-Safety Policy

Computing and E-Safety Policy

Contents

Computing and E-Safety Policy Rationale

St Mary's C of E School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at St Mary's C of E School want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote student achievement following the National Curriculum and Early Years Foundation Stage Curriculum.
- Develop the curriculum and make learning exciting, purposeful and support problem solving.
- Enable students to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding of how computing is used in the world around us.

E Safety Policy

To enable our aims to happen we have taken a whole school approach to E-safety, which includes the development of policies and practices, the education and training of staff and students and the effective use of the School's computing infrastructure and technologies.

Safeguarding children from all risks of harm is an important part of a school's work and protecting them from extremism is one aspect of that. New statutory duties were placed on schools by the Counter Terrorism and Security Act 2015 which means they must work to prevent children being drawn into extremism. we ensure that through our vision, values, relationships and teaching we promote tolerance and respect for all cultures, faiths and lifestyles. The Governors also ensure that this ethos is reflected and implemented effectively through school policy and practice and that there is an effective suite of safeguarding policies in place to safeguard and promote pupils' welfare.

St Mary's C of E School as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all students using computing technology. We recognise that computing can allow disabled students increased access to the curriculum and other aspects related to learning.

St Mary's C of E School is committed to ensuring that **all** its students will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.

Scope of Policy:

The policy applies to:

- all students;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

St Mary's C of E School will ensure that the following elements are in place as part of its safeguarding responsibilities to students:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of students when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- a reporting procedure for abuse and misuse.

Infrastructure and Technology

St Mary's C of E School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is ICT4 who provide our Broadband Access as well as filtering capability. As part of our commitment to partnership working, we fully support and will continue to work with ICT4 to ensure that student and staff usage of the Internet and digital technologies is safe.

St Mary's C of E School will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that sees the welfare of the child as paramount. To this end, we expect any organisation using the school's computing or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

Policies and Procedures

We at St Mary's C of E School understand that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist within St Mary's C of E School are aimed at providing a balance between exploring the educational potential of new technologies safeguarding students. St Mary's C of E School will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

St Mary's C of E School expects all staff and students to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's computing facilities and digital technologies.

<u>Users shall not:</u>

Visit Internet sites or use email to, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material

[1] For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and also permission is given by senior leaders, so that the action can be justified, if queries are raised later.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 18 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist, homophobic or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

In addition, users may not:

- Use the ICT4 or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves ICT4 or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of St Mary's C of E School or the ICT4.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of St Mary's C of E School or ICT4;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via ICT4.

- Undertake activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible via the St Mary's C of E School network and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the St Mary's C of E School network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - other misuse of the St. Mary's network, such as introduction of viruses.
    - Use any mobile or digital technologies 3G or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Staff/ Employees may use the Internet and e-mail for personal use providing that:

- Personal use is only outside normal working hours and for limited periods
- users make it clear in e-mail to the recipient that it is not sent by the user in their capacity as a representative of the school.

Regular, extensive personal use will normally result in disciplinary action. Emails sent in the capacity of a representative of the school must be sent from a school e-mail address. Personal e-mails should not be received in your school e-mail inbox.

Where St Mary's C of E School or ICT4 become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

Reporting Abuse

There will be occasions when either a student or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the student or adult should be report the incident **immediately** following the reporting procedure (Appendix 1).

The School also recognises that there will be occasions where students will be the victims of inappropriate behaviour that could lead to possible or actual significant harm. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person (DSP) for Child Protection within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Services and the Police. The DSP for St Mary's C of E School is Mrs. D. Jones, Headteacher.

The School, as part of its safeguarding duty and responsibilities will, in accordance with SWCP Procedures assist and provide information and advice in support of child protection enquiries and criminal investigations.

Education and Training

St Mary's C of E School recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

As part of achieving this, we want to create within St Mary's C of E School an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our students to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

To this end, St Mary's C of E School will:

- Enable all students to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support students in gaining positive experiences when online and can help students develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

Standards and Inspection

St Mary's C of E School recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to students are minimised.

Website Guidelines

A website can celebrate good work, promote the school, publish resources for projects and homework, and link to other good sites of interest. No names and photographs that identify individual children will appear on it. Home information and e-mail identities will not be included only the point of contact to the school (ie telephone number, school address, e-mail to the Headteacher/Co-ordinator). Group photographs will not contain a list of names. Work displayed will be of the highest quality and reflect the status of the school.

Monitoring

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a student or member of staff may have. St Mary's C of E School recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

With regard to monitoring trends, within the school and individual use by school staff and students, St Mary's C of E School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

Another aspect of monitoring, which our school will employ, is the use of mobile technologies by students, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our students, and where necessary, support individual students where they have been deliberately or inadvertently been subject to harm.

Sanctions

St Mary's C of E School has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

- Child / Young Person
    - The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of Internet and email being withdrawn.
    - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- Adult (Staff and Volunteers)
    - The adult may be subject to the school's disciplinary process, if it is deemed he/she has breached the policy
    - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

If inappropriate material is accessed, users are required to immediately report this to the Headteacher or Computing Coordinator so this can be taken into account for monitoring purposes.

Working in Partnership with Parents and Carers

St Mary’s C of E School is committed to working in partnership with parents and carers and understand the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

We at St Mary’s C of E School also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

Computing Policy

To enable our aims (page 3) we have a whole school approach to teaching computing skills both in computing lessons and in cross curricular learning. These skills will include:

Key stage 1

Pupils should be taught to:

- understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key stage 2

Pupils should be taught to:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour including extreme and radicalising behaviour; identify a range of ways to report concerns about content and contact.

Teaching and Learning

Activities are planned from the Switched on to ICT scheme of work, taking into account the different levels of children's skills and building on previous knowledge. This scheme ensures coverage of both the skills and techniques in the National Curriculum (stated above) and the development of computing capability by applying computing within the context of other subjects. All children will have computing experiences indoors, outdoors and through role play in both child initiated and teacher directed time.

Computing is delivered through a variety of teaching and learning methods e.g. whole class, group and individual work. Differentiation and progression are ensured by a variety of approaches such as:

- Same activity but different expectations of outcome
- Same theme but different levels of input
- Allowing for different pace of working
- Different groupings of children
- Developing different modules of work at different times of the year for different abilities

Computing will be integrated into all other subjects at appropriate stages and used as a tool to enhance other learning. In addition we also teach the skills and knowledge of computing as a subject in its own right.

Working on the Internet requires a mature and responsible attitude. The school aims to develop this attitude and has:

- A code of conduct as part of the home school agreement signed by parents and pupils.
- Acceptable Use Rules, signed by children and adults in each class every September.
- A clear E safety guidelines and procedures set out earlier in this policy.

Assessment

Assessment of computing will take place within all curriculum areas, however, clear learning objectives will support the focus of assessed activities. Pupil achievement will be recorded in an individual computing record and held, with evidence, in a class computing file on the server.

Management

There is a designated computing co-ordinator to oversee the planning within the school. The co-ordinator will be responsible for informing the rest of the staff about new developments and where appropriate for organising (and providing) appropriate training. The computing co-ordinator will not be a technician but will advise colleagues on managing equipment and software in the classrooms. A central resource area will be maintained and reviewed annually along with other resources for computing.

The co-ordinator will monitor the curriculum and report to the Headteacher on progress in accordance with the School Development Plan/School Self Evaluation Form.

Inclusion

The school recognises the advantages of the use of computing by children with special educational needs. Using computing can:

- Address children's individual needs
- Increase access to the curriculum
- Enhance language skills

Equal Opportunities

We ensure computing is accessible to all children in full accordance with the school's Equal Opportunities policy.

Health and Safety

All equipment will be checked annually under the 'Electricity at Work Regulation 1989'.

The Health and Safety at Work Act (January 1993) European Directive deals with requirements for computer positioning and quality of screen. This directive is followed for all administration staff. Whilst this legislation only applies to people at work we seek to provide conditions for all children which meet these requirements.

Provision

There are 24 networked machines in the Computing suite. In a mobile laptop trolley there are an additional 25 laptops. There are a set of netbooks, 18 kindles and 24 iPad2. Every classroom has a digital project and smart board, including the Computing suite. Each teacher has a laptop, flip-cam and digital camera.

Resources are purchased and deployed effectively to meet the requirements of the Early Years Foundation Stage Curriculum and National Curriculum.

The main staff INSET will take place when computing is the priority on the school development plan. However in-service training may also be a part of staff meetings, if appropriate. This will include:

- Introduction of software
- General training for computing
- Whole school support in planning for computing sharing ideas
- Sharing children's work
- Moderation of children's work

Opportunities for training are offered wherever possible, to meet whole school needs as well as those of individual teachers.

Other than within the limited exceptions allowed for in legislation - this school will not discriminate against children or with regard to how pupils are treated, on grounds of sex, race, disability, religion or belief. This includes discrimination in provision of teaching or allocating the pupil to certain classes, applying different standards of behaviour, dress and appearance, excluding pupils or subjecting them to any other detriment, and conferring benefits, facilities or services.

Appendices of the Computing and E-safety Policy
There are multiple aspects of the school's Computing and E-safety policy, which include:

- Flowchart for reporting.
- Legal Compliance Policy.
- Computer access policy.
- Home Internet Use agreement

These appendices will be reviewed annually along with the Computing and E-safety Policy.

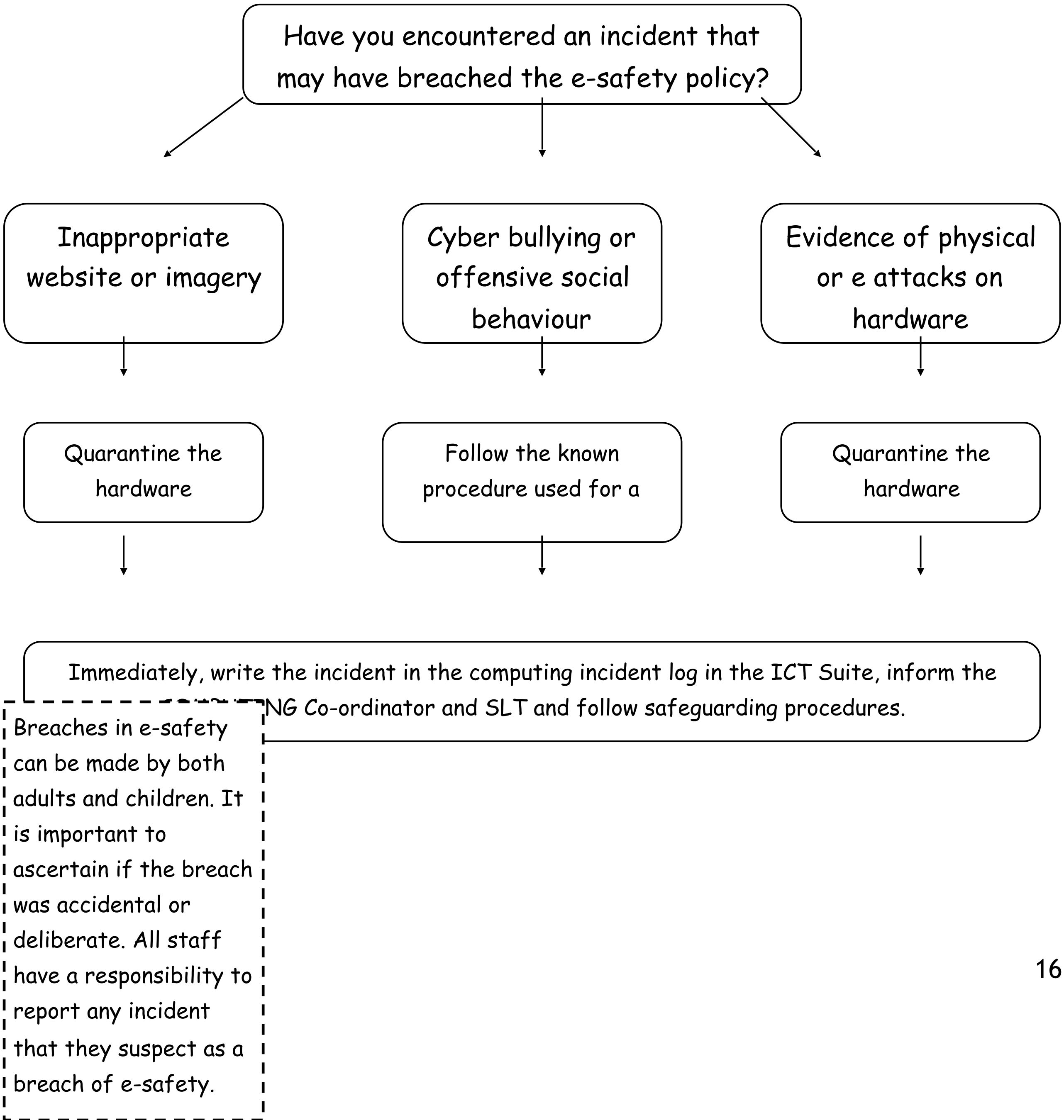
Signed ………………………………………………………………. Dated …………………………….

(Chairman of Governors)

Signed ……………………………………………………………… Dated ……………………………

(Headteacher)

Appendix 1 (Reporting Flow Chart)



Have you encountered an incident that may have breached the e-safety policy?

Inappropriate website or imagery

Cyber bullying or offensive social behaviour

Evidence of physical or e attacks on hardware

Quarantine the hardware

Follow the known procedure used for a

Quarantine the hardware

Immediately, write the incident in the computing incident log in the ICT Suite, inform the COMPUTING Co-ordinator and SLT and follow safeguarding procedures.

Breaches in e-safety can be made by both adults and children. It is important to ascertain if the breach was accidental or deliberate. All staff have a responsibility to report any incident that they suspect as a breach of e-safety.

Appendix 2 (Legal compliance Policy)

Introduction

This policy aims to ensure that St Mary's C of E School's software is licensed, that software is not unlawfully copied and that employees and others will access to the school's computer systems are aware of their responsibilities. It also describes how the school will seek to achieve these aims.

Copyright

Copying software is subject to the same law of copyright as printed documents. These laws exist to protect copyright holders who may claim damages if their rights are infringed: the unauthorised copying of software may also lead to criminal charges if it materially affects a copyright holder's interests.

Definitions

"Software" is defined as a "set of machine readable instructions which are capable of causing a computer to indicate, perform or achieve a particular function". It includes:

- Propriety software e.g. Microsoft products
- Screen savers
- Games
- Shareware
- Coverware – software obtained from internal bulletin boards
- Any file with an EXE suffix

"Copying" includes the electronic copying of information

Purchasing, Licensing and Developing Software

All software must be licensed and the school will maintain an up-to-date register of software purchased for use on the school's computer. Licenses and original software disks for non-corporate software will be retained by the Computing co-ordinator.

Where required for licences that allow concurrent use, the school will ensure concurrency control software exists on fileservers. The school will also implement routines to check concurrency for software operating on multiple fileservers and will alert users to any potential licence infringements.

Copying/Installing Software

Software of any description may only be copied or imported onto systems by employees who have been specifically authorised to do so. This applies to all software, including software obtained from on-line services, the Internet, magazine covers or from colleagues or friends.

The school's software must not be used on privately owned equipment without written approval being obtained from an authorised member of staff who must be satisfied that the terms and conditions of any license are being complied with.

Privately owned software must not be installed on the school's fileservers in any circumstances.

Privately owned software may be installed on non-networked computers but only with the prior written approval of an authorised member of staff who must be satisfied that such software is appropriately licensed.

Audits

A software audit will be undertaken each year by the school, in addition to which random audits may be performed in order to verify the County Council's compliance with copyright law.

Electronic audit tools will be used to automatically compare software installed on computers with the software register. The outcome of annual audits will be reported to the Management Board.

Responsibilities

The Computing Co-ordinator will be responsible for:

- Ensuring compliance with this policy
- Ensuring that all relevant employees, agency staff and others with access to the school's computer systems are aware of this policy
- Ensuring that software and software development is purchased in accordance with the County Council's Corporate Information Management Strategy
- Ensuring that computer equipment is disposed in accordance with the County Council's Corporate Information Management Strategy
- Addressing any breaches of this policy in accordance with personnel procedures

Generally the school will take measures to promote an awareness of this policy.

Breaches of Policy

Breaches of copyright could result in serious financial penalties for the County Council, including the possibility of criminal prosecution.

To safeguard the County Council and school's interests, therefore, employees acting in breach of this policy may be subject to disciplinary action under the County Council's Disciplinary and Capability Procedure or, in the case of uninformed members of the Fire Brigade, the Fire Service (Discipline) Regulations 1985.

Safe working practices for computer projectors

The following procedures apply to staff, students and visitors.

- Never stare into the projector beam
- Where possible, avoid standing directly in the path of the beam and where unavoidable, stand with your back to the source of the beam
- If children are working at the IWB, staff should ensure that the audience is positioned so that when the presenter is addressing them, they are not looking into the beam
- Staff supervising children where projectors are being used, should ensure that children are aware of, and observe the safe working practise
- To minimise the required lamp power, use window blinds where available
- When not using the projector for any length of time, switch off to maximise lamp life and minimise accidentally looking into the beam

This school is firmly committed to equality and diversity.

Other than within the limited exceptions allowed for in legislation - this school will not discriminate against children or with regard to how pupils are treated, on grounds of sex, race, disability, religion or belief. This includes discrimination in provision of teaching or allocating the pupil to certain classes, applying different standards of behaviour, dress and appearance, excluding pupils or subjecting them to any other detriment, and conferring benefits, facilities or services.

Appendix 3 (Computer Access Policy)

Document purpose

The Computer Misuse Act of 1990 created several offences in relation to unauthorised access to computer systems and stipulates penalties of prison sentences. By following the policy below staff will avoid disciplinary action and possible criminal prosecution.

The purpose of this Policy is to ensure adequate control over the access to Cornwall County Council's computer based information, programmes and processes, and to reduce the risk of unauthorised access to Council information, in electronic or paper format, which may be derived from Council computer networks.

Scope

This policy applies to all Council employees using Council computer information and systems, including those working from home or non-Council locations. In exceptional circumstances, the measures outlined in this Policy may compromise the operational running of business services. These cases may be referred to ISG, for guidance, on an individual basis to ensure business continuity with departmental systems without jeopardising overall network security.

Computer Access

Access to all Council systems is through a sign-on procedure, unique to the individual, which requires a user password before access to shared resources is permitted. Incorrectly entered passwords will lock out access on the third incorrect attempt. Under these circumstances access can only be released by the Systems Administrator.

Council computer equipment may be procured, approved and appropriately configured by ISG unless there are exceptional circumstances.

Access to the Council's corporate network through public connections will be protected by passwords and by employing safeguards against unauthorised interception. Likewise, for access to public data from the Council's corporate network.

Users level of access will be agreed by a recognised manager within their department, who will be responsible for ensuring all user access levels are appropriate and ISG will arrange user access levels in accordance with their instructions.

This Policy should be read in conjunction with the Council's other computer related policies, of which users will be aware.

Management of user access

Where a user requires access to resources beyond their current level of access, this may be arranged by the Systems Administrator, on receipt of proof of authorisation by the relevant manager from the department recognised for these purposes.

Users must keep their passwords confidential and secure and must change them regularly, at least once a month, and in any event where the secrecy of their password may be compromised. To reduce easy identification by hackers, passwords should be a minimum of 6 characters (a mixture of letters and numbers) which do not represent a repeatable sequence, dictionary word, or names of partners, children, etc. Written lists of passwords and log-on procedures may jeopardise the security of the systems and must therefore be kept secure at all times. In the event of a password being forgotten, ISG Systems Administrator may issue a new one on request. Proof of user identification and authorisation will be required in these circumstances. Screen saver passwords will be used to protect the confidentiality of information on workstations left inactive.

All requests for creation, amendment or deletion of corporate information or network access to it, including password control, must be requested through the formal change control procedure managed by ISG.

Network Access

Access for approved third party support organisations or teleworkers is available through secure dial-up connections, as configured by ISG. Temporary workers, teleworkers and contractors will have access to the necessary systems through a unique sign-on procedure which will be removed at the end of their employment.

Modem access from the Council's corporate network to public networks is not permitted as this method by-passes the Council's security equipment. In the event of a genuine business requirement for such access, ISG may be consulted on the option of controlled modem access to public networks.

Mobile Computing

Users of lap-top and other forms of mobile computers should protect any sensitive information copied to a local system by password. Highly sensitive information must be protected by disk encryption.

Users of mobile computers and phones should avoid any risk of security from eavesdropping by using the equipment in an appropriate location. These items of equipment should be suitably stored to reduce the risk of theft or vandalism.

Specific Responsibilities

All Council network configuration and access management will be undertaken by ISG to meet user-defined requirements.

Access to applications outside of the users access level may be obtained by approval from the person with day-to-day responsibility for the system.

System Administrators are required to adhere to the Council's guidelines on system configuration and administration, and will produce regular reports to management on authorised users.

Managers are responsible for maintaining up-to-date information on authorised users through the starter/leaver process, and updates on user access identified from access reports produced by System Administrators.

Users are responsible for conforming to the password policy.

It is the responsibility of the recognised Departmental Manager to authorise access to their systems.

Review

This policy will be reviewed annually or in the light of changed circumstances.

Key Contact

ISG Director at County Hall, Truro

Appendix 4 (School Internet Agreement)

<u>St Mary's School Home –School Internet Agreement</u>

This document is to be read through with your parents/ carers and then signed.

- At St Mary's School, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes materials they choose to access, and language they use
- Pupils using the Internet or computing devices are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally they are expected to report it immediately to a teacher.
- Pupils are expected to use polite, respectful language in their online and e-mail communications both at school and at home. They should only contact people they know or those the teacher has approved.
- Pupils must ask permission and be supervised before accessing the Internet or computing devices at school.
- Pupils must ask permission to access other people's files.
- Computers in the school should only be used for schoolwork and homework unless permission has been granted otherwise
- Pupils must ask permission to download to a computer from the Internet
- Pupils must ask permission to use data sticks or CD-ROMs brought in from home for use in school
- Homework completed at home may be brought in on data sticks or CD but this will have to be virus scanned by the class teacher before use
- Personal printing is not allowed on our printers for cost reasons (e.g. pictures of pop groups/cartoon characters)
- Pupils are educated to protect their personal information such as telephone numbers and addresses online by never giving them out.
- Pupils consistently choosing not to comply with these expectations will be warned and subsequently, the behavioral policy and sanctions will be applied.

I have read through this agreement with my child and agree to these safety restrictions

Signed ……………………………………………………………….

(Parent/carer)

Name of child ……………………………………………………………….

Child's signature ……………………………………………………………….

St Mary's C of E School
Higher Trehaverne
Truro
Cornwall
TR1 1RJ
(Telephone: 01872 276689)
(E-mail: secretary@st-marys-truro.cornwall.sch.uk)

Dear Parents

Responsible Use of the Internet and Computing Devices

The school has a number of devices which give the children access to the Internet.

Mindful of the problems there are with children gaining access to undesirable materials, we have taken steps, along with the Local Authority to deal with this.

Our Internet access is supplied by ICT4 (an award winning filtering company). It has a built in filtering system that restricts access to sites containing inappropriate content. All our screens are in public view and an adult is present to supervise.

No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material. We have been assisted by the LA to inform you of the rules which the children are expected to follow to help with our precautions. Children should continue to benefit enormously from this facility and have on the whole been using it very responsibly already.

I would ask you to look through these rules and discuss them with your child and then return the signed form to us at school. If you would like to have a look at our full 'E safety policy', I will be more than willing to forward you a copy – particularly by e-mail as this is cost free to the school. The school's e-mail address is available at the top of this letter.

Yours sincerely

Mrs. L Stevenson M Ed

Computing and Assessment Coordinator