Information & communication technology policy

E-Safety Overview [1]

Harnessing Technology: Transforming learning and children's services [2] sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Green Paper *Every Child Matters*[3] and the provisions of the *Children Act 2004*[4], *Working Together to Safeguard Children*[5] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- Safe from maltreatment, neglect, violence and sexual exploitation.
- Safe from accidental injury and death.
- Safe from bullying and discrimination.
- Safe from crime and anti-social behaviour in and out of school.
- Secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

---

[1] **The e-Safety Policy has been written and adapted by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance.**

[2] **http://www.dfes.gov.uk/publications/e-strategy/**

[3] **See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]**

[4] **See Every Child Matters website [http://www.everychildmatters.gov.uk]**

[5] **5 Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]**

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The Technologies:

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (e.g. www.msn.com, www.google.com, www.whatsapp.com) often using simple web cams
- Blogs (e.g. an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (e.g. www.facebook.com , www.myspace.com , www.twitter.com , www.bebo.com, www.hi5.com)
- Video broadcasting sites (e.g. http://www.youtube.com/ , www.vimeo.com)
- Chat Rooms (e.g. www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (e.g. www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (e.g. http://www.apple.com/itunes/ , http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications
- Photo sharing sites (e.g. www.instagram.com, www.flickr.com , www.pinterest.com).

Whole school approach to the safe use of ICT:

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools.
- Policies and procedures, with clear roles and responsibilities.
- A comprehensive e-Safety education programme for pupils, staff and parents.

Reference: Becta - E-safety Developing whole-school policies to support effective practice[6]

Roles and Responsibilities:

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school, including public facing technology. Any communications made about staff, pupils or the school on public facing technology could result in sanctions or details being given to the police. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the ICT Learning Leader and the Child Protection Team.

[6] http://schools.becta.org.uk/index.php?section=is

Our school **e-Safety Co-ordinators** are: Karen Calamaro, Sunil Pindoria and Russell Davey.

Our school Child Protection Officers are: Allyson Moss and Kay Johnson.

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[7]. The school's e-Safety coordinator ensures the Head, senior management, Governors and staff are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance[8] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail.
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
- Publication of pupil information/photographs and use of website.
- eBullying / Cyberbullying procedures.
- Their role in providing e-Safety education for pupils.

Staff are reminded / updated about e-Safety matters at least once a year.

How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-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.

The school provides digital cameras for use in school, the memory from which should be cleared regularly, preferably daily, to prevent images of staff and pupils being accessed by others outside school without permission. The taking of photos or video on personal devices, such as mobile phones, is not permitted. Permission can be sought from a member of the ICT Team to use personal devices in emergency circumstances only, and all images / videos must be removed immediately on return to school. The ICT Team may request to see devices have be cleared of such images.

Infringement upon these rules is taken very seriously with possible sanctions being implemented, see below.

[7] http://www.ceop.gov.uk/

[8] Safety and ICT - available from Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview / counselling by Key Stage Leaders / Village Leaders / Class Teachers / e-Safety Coordinators / Head Teacher.
- informing parents or carers.
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.
- referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the head teacher.

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.

Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. This is to be encouraged at TVS, where ability allows. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems.

In support of this, the government provided a Standards Fund grant to support Local Authorities procure broadband services through local Regional Broadband Consortia (RBC). We now access the internet through BT NET and maintain our own filtering service.

The Risks:

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

Schools also need to protect themselves from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to

'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Schools help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised" and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff.

Technology:

Schools should be connected to the NEN through their RBC. At TVS we maintain our own internet filtering software, anti-spamware and anti-virus software, which we regularly update. Additionally, we also use Impero on all our devices to monitor software use and to track equipment location. Monitoring occurs at different times throughout the day.

Unfortunately, inappropriate materials will inevitably get through any filtering system. So, schools should be vigilant and alert so that sites can be blocked. Conversely, sometimes appropriate websites need to be unblocked. The Network Manager manages the filtering policy for the school and the LA will usually be able to provide them with advice and back-up. All internet activity is logged by the school's Barracuda Web Filtering System. These logs may be monitored by authorised The Village School staff.

The TVS network has regular 'health' checks, conducted by The ICT Team on their scheduled once fortnightly visit, to ensure we have the latest versions of patches and service updates. The ICT Team checks shared areas on the network and conducts annual audits to check hardware and software usage. Any inappropriate applications on the network are reported to The ICT Team and removed. Individual log-ins, coupled with Auditing software, means activity on the network can be monitored and logged. High level monitoring of website access is also undertaken by Virgin Media and logs can be obtained where a site is under investigation.

Filtering, coupled with child-friendly search engines [e.g. http://yahooligans.yahoo.com/ | www.askforkids.com/] reduce the likelihood of children finding inappropriate materials. Schools should set-up search engines so that 'safe search' is turned on. TVS uses Google as its default search engine.

TVS staff have been made aware that they should not send personal data across the Internet unless they know the person / organisation they are sending it to, and parental / caregiver permission must be gained.

Internet Policies:

This school:

- Maintains broadband connectivity through BT NET
- Works in partnership with the LA to ensure any concerns about the system are monitored so that systems remain robust and protect students.
- Ensures network health through appropriate anti-virus software etc and network set-up.
- Ensures their network is 'healthy' by having regular health checks on the network conducted by The ICT Team.

- Ensures the Network Manager and the ICT Team are up-to-date with network services and policies.
- Ensures the Network Manager and the ICT Team check to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately.
- Uses individual logons for staff and some pupils, where appropriate.
- Never sends personal data over the Internet unless the person / organisation is known to the sender, and that permission is gained from the parents / caregivers.
- Ensures teachers and Teaching Assistants never allow pupils to use the internet unsupervised or to use a computer without a responsible adult being present. All websites used for teaching should be checked prior to using them with the class.

Procedures for teaching and learning

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. Supervision is the key strategy. Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation. A teacher or Teaching Assistant should be with pupils whenever they use the internet and pupils should always be under supervision when using any computer.

Surfing the Web:

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"
Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. Of course the experienced teacher will choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand.

Pupils do not need a thousand websites on weather. A small selection may be quite enough choice. Using the 'favourites' list is a useful way to present this choice to pupils. There may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing, for example, to a pornographic one, therefore sites should always be previewed prior to use in any teaching situation.

Search Engines:

Some common Internet search options are high risk, for example Google image search. Our school chooses to keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution.

Video Conferencing:

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. Webcams are generally not used at TVS for meetings, but any that are used would require support from our ICT Team to ensure safety.

Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to, adult material. In schools adult sites would normally be blocked

but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

Podcasts:

Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments.

Sanctions and Infringements:

The school's ICT Acceptable Usage Policy is made available and explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age, ability and role. In signing this document, staff and pupils will be aware that there are possible sanctions for infringements. See the ***Infringements and possible sanctions*** section of this document for further details.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be referred at the earliest opportunity to the local police station. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.

Teaching and Learning Policies:

This school:

- Supervises pupils' use of the internet at all times, as far as is reasonable.
- Uses an in house filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature.
- Encourages staff to preview all sites before use [where not previously viewed and cached], or to use sites accessed from managed 'safe' environments such as the Learning Platform.
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search.
- Informs users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT Team. Our systems administrators report to LA where necessary.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only uses video conferencing activities monitored by the ICT Team.
- Only uses approved or checked webcam sites.
- Has blocked access to music download or shopping sites – except those approved for educational purposes.
- Requires pupils and their parent/carer to individually sign an acceptable use agreement form which is fully explained and used as part of the teaching programme, where appropriate.
- Requires all staff to sign an acceptable use agreement form and keeps a copy on file.

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system.
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form, where appropriate.
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents / carers.
- Immediately refers any material we suspect is illegal to the appropriate authorities – LA / police.

E-safety Policies:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or ICT Team.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident.
- Will teach e-safety, following guidance from the LA or London / national grid guidance, where appropriate for the ability of the individual pupil. Pupils should be taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
    - to discriminate between fact, fiction and opinion
    - to develop a range of strategies to validate and verify information before accepting its accuracy
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
    - to know some search engines / web sites that are more likely to bring effective results
    - to know how to narrow down or refine a search
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - to understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour
    - to not download any files – such as music files - without permission
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos
    - to have strategies for dealing with receipt of inappropriate materials
- 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 observe and respect copyright / intellectual property rights.
- Makes training available to staff on the e-safety education program.
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information in safety leaflets; in school newsletters; on the school web site
    - suggestions for safe Internet use at home
    - provision of information about national support sites for parents

Managing E-Mail

How will e-mail be managed?

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects.

Technology:

All e-mails in the school Gmail system go through a filtering process for inappropriate language regardless of whether they are in safemail or not. Also, all communications within school are subject to monitoring for safeguarding.

Where the school receives nuisance or bullying e-mails and the e-mail address of the sender is not obvious, it is possible to track the address using 'e-mail' tracking software.

Procedures:

In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses, such as Hotmail, is discouraged by the school for all professional purposes. All teaching staff, other staff members, classes or pupils where appropriate will be given a school email account by the ICT Team. Anyone using a school email account will be expected to sign the ***ICT Acceptable Usage Policy Form.*** Staff email addresses will be grouped by department, teaching area, etc, to aid the sending of multiple emails and to avoid unnecessary printing.

Education:

Pupils and staff need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's e-Safety and anti-bullying education programme and will be taught where appropriate, according to ability.

Email Policies:

This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.tvs.sch.uk / head@schoolname.tvs.sch.uk for any communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.
- Accounts are managed effectively, with up to date account details of users.

Pupils:

- Pupils will be monitored at all times when using email.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work, where appropriate.
- Where appropriate, pupils can be introduced to the principles of e-mail through closed 'simulation' software.
- Where appropriate, pupils will be taught about the safety and 'netiquette' of using e-mail i.e.
    - Not to give out their e-mail address unless it is part of a school managed project or 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.
    - The sending of attachments should be monitored by the class teacher.
    - 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 ***ICT Acceptable Usage Policy 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 use their school email accounts for professional purposes.
- E-mail sent to an external organisation should 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 attachments is permitted, but they should bear in mind that personal documents are confidential and should only be sent to LA departments / colleges etc where consent has been given by the parent / carer.
    - the sending of chain letters is not permitted.
- Staff sign the ***ICT Acceptable Usage Policy Form*** to say they have read and understood the e-safety rules, including e-mail and understand how any inappropriate use will be dealt with.

Using Digital Images and Video Safely

Developing safe school web sites:

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Sean Jeffrey, Data Manager, will oversee the school's website content and will be the only person with the authority to upload content. He will liaise with the Head Teacher, Key Stage leaders, Village Leaders, teachers and the ICT Team regularly to discuss content, updates and the general upkeep of the website. The Head

Teacher will have the final say in anything that is to be uploaded onto the website and will be shown all content prior to any uploads.

Use of still and moving images:

The use of photographs and video footage is an integral part of TVS's recording and assessment procedures. Where photos / video footage are to be used on the website, consent will be gained from parents / carers prior to any uploading. Where appropriate, group photographs rather than photos of individual children will be used. Where individual pupil's images are to be used, camera angles or digital techniques will be used to disguise the identity of the individual. Only first names will be used, if necessary, and only if their image is not used. When a photograph / video footage is used of a pupil, their name will not be used to reduce the risk of inappropriate, unsolicited attention from people outside the school.

If the website is showcasing examples of pupils work only their first names, rather than their full names, will be used.

Only images of pupils in suitable dress will be used to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken and parental permission be gained

Parental permission will be obtained in writing before publishing any photographs, video footage etc of pupils on the school website or in a DVD. This ensures that parents are aware of the way the image of their child is representing the school.

Procedures:

Excerpts of pupils' work can be used on the website rather than digital images of the individual, such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked prior to inclusion on the school website to ensure that the content is appropriate both to the school and for the intended audience. All links will be checked regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils will be reviewed before publishing it on the school website, making sure that the work does not include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them.

Content will also be checked to avoid infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

Any guest books, notice boards or blogs on the school's website will be monitored to ensure they do not contain personal details of staff or pupils and the content is appropriate.

Any webcam use on the school's website will be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If the website is showcasing school-made digital video work, care will be taken to ensure that pupils are not referred to by name on the video and that pupils' full names are not given in credits at the end of the film.

Staff should not to use their personal phone during school hours, where they are in contact with pupils. The use of personal cameras is discouraged and should not be used without permission from the Head Teacher. If personal equipment is being used it should be registered with the school and a clear understanding that photographs will be transferred to the school network and will not be stored at home, on memory sticks or used for any other purpose than school approved business.

Technical:

Digital images / video of pupils will be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.

When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web. [An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be viewed by reading the code of the website.]

Staff must not use software to 'rip-out' sections of copyrighted movies without permission.

Education:

Staff and pupils should know who to report any inappropriate use of images to and understand the importance of safe practice. In this case, this would be the ICT Learning Leader, the ICT Team, the Child Protection Team or the Head Teacher.

Using the School Network, Equipment and Data Safely: general guidance

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

Network Setup:

Each classroom and each specialist area has a PC which is connected to the network. Specialist equipment such as switches, communication aids etc are added to each PC where necessary to suit the needs of the class and to encourage the use of ICT in the classroom. Additional standalone PCs are being added to classes where appropriate to provide additional access to additional resources and to encourage more appropriate use of ICT equipment.

A range of software is available on the network, with some classes having access to additional, more appropriate software where necessary. *Communicate: In Print* and *Grid 2* software is widely used throughout the school as aids to reading, for PECs work and also for creating resources.

The network structure itself was completely overhauled in since the merger to help improve the use of ICT throughout the school and to encourage sharing of resources. The network consists of several areas: *Individual home drives (My Documents)*, *Staff Area*, *Class Folders*, *Pupil Work*, *Media*.

Users are split into two categories: *staff* and *pupils*. Staff have access to their own personal 'My Documents' folder that has restricted access for that specific user. Staff can access class folders. Pupil logons also have their own personal 'My Documents' folder that has restricted access to *Class Folders* and the *Resources* folder in the *Staff Area*.

Staff Area is a shared area for staff to use, containing student documents, templates, training documents, policy documents etc. Pupils have restricted access to the *Resources* folder.

Class Folders is where staff and classes can share documents that are for training use or private, such as Annual Review documents.

Pupils Work is where pupil documents and photos are stored. Pupils have restricted access to this area.

Media is a shared area that everyone can access to use and store large media files and old photos from both schools prior to the merger.

The administration network is kept separate. Restricted access is given to the Administration Team and the SLT.

Network Policies:

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy (included in the Acceptable Usage Policy). Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password.
- Provides pupils where necessary with an individual network logon username and password.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find.
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network.
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles.
- 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. Computers and projectors are set to switch off automatically at the end of the school day.

- Has blocked access to music download or shopping sites – except those approved for educational purposes.
- Makes it clear that there are copyright laws regarding the internet and staff must seek permission from the creator where appropriate prior to use in resources / teaching.
- Makes it clear that school computers should not be used to make payments for purchases online, unless sanctioned by the Head Teacher. Any use of credit cards on school computers will be at the risk of the user and the school does not accept any responsibility for any problems that may occur.
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies.
- Maintains equipment to ensure Health and Safety is followed. E.g. projector filters cleaned by ICT Team, equipment installed and checked by approved Suppliers / LA electrical engineers.
- Has separate curriculum and administration networks, but access between servers is provided where appropriate to ensure staff users can only access modules related to their role.
- Remote access is available through a restricted portal. The ICT Team will provide details on request.
- 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.
- Ensures that all personal data sent over the internet is only sent within the approved secure system in our LA.
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Reviews the school ICT systems regularly with regard to security.

Laptop and Mobile Equipment: general guidelines

Teaching staff are provided with laptops, financed through school funds. Updated models will be given out to staff, finances permitting, when older models become obsolete or unusable.

Laptops / tablets should be signed for by the teacher (***ICT Equipment Acceptable Usage Policy Form***), making clear that they are responsible for the equipment on loan to them by the school for use solely to support their professional responsibilities and that they should notify the school of any "significant personal use" as defined by HM Revenue & Customs.

Laptops / tablets should be returned to school for regular anti-virus updates and should not be connected to external networks without consultation with the ICT Team.

Laptops / tablets loaned to teachers by the school should be returned to the school prior to leaving their post at the school.

Safeguarding and Protecting Children[9]

All staff should go to one of the following staff members if they have a concern that a child or young person might be at risk or suffering harm as a result of the use of ICT and the internet technologies:

- ICT Learning Leader.
- Child Protection Team.
- ICT Team
- Head Teacher.

[9] This section has also been included in the Child Protection Policy

"As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. *Report to and discuss with a named child protection officer in school and contact parents*
2. *Advise the child on how to terminate the communication and save all evidence*
3. *Contact CEOP http://www.ceop.gov.uk/*
4. *Consider the involvement police and social services*
5. *Inform LA e-safety officer*

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear. "

How will infringements be handled?

Whenever a student or staff member infringes the ICT Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Staff

Category A infringements (Misconduct):

- Excessive use of internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

*[Sanction - **referred to Village Leader / Headteacher**. Warning given.]*

Category B infringements (Gross Misconduct):

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988.
- Bringing the school name into disrepute.

*[Sanction – **Referred to Headteacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police]*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.

- Instigate an audit of all ICT equipment by the ICT Team - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

The school is likely to involve external support agencies as part of these investigations e.g. the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

They will be fully explained and included within the school's ICT Policy. All staff are required to sign the school's *ICT Acceptable Usage Policy Form*.

Pupils will be taught, where appropriate, about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'.

The school's ICT Policy will be made available and explained to parents, where necessary. Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.

ICT problem reporting

The ICT Learning Leader can be approached to discuss / resolve minor ICT problems, software support etc, however it should be noted that her role is primarily a class teacher and teaching her class is her highest priority. Teachers are advised that they should not interrupt the ICT Learning Leader's lessons unless there is an urgent problem. Teachers are also advised that is it is good practice to check out any websites used in their teaching in advance (taking into account the school's internet safety policy) and check that equipment is working prior to a teaching session.

To report general ICT problems (e.g. installing new software, printer problems, lack of internet access etc) a description of the problem should be written down in the ICT Help Desk, accessible from the school intranet. The ICT Team check the fault log on a daily basis. Updates on any ICT problems can be gained via automated emails and by checking the ICT Help Desk.

Ink is refilled into the networked printers by an external company, who monitor the printers /photocopying system daily

For any problems that are deemed urgent, e.g. pornographic websites being allowed through the filter etc, the ICT Team should be informed immediately.

If there is any confusion about how to report a problem, please speak to a member of the ICT Team.

Interactive whiteboards

TVS uses BENQ interactive boards. Each IWB is now a plasm scree, so there are no costly projector bulbs to replace. This also means that there is no visual interference from shadows. The IWBs are also multi-touch and can work interactively with tablet devices. Regular checks are made by the ICT Team to ensure equipment is working correctly.

Recycling

TVS is committed to recycling any computer related hardware in accordance with regulations set out by the government. No equipment, no matter how small, is thrown out with the usual waste, but is instead collected together for appropriate recycling through schemes approved by Brent. TVS has registered with an approved company for the collection of old / broken hardware.

Programmes of study

ICT is embedded throughout the curriculum at TVS in all Key Stages. The main focus is to promote communication, with the introduction of communication aids as appropriate. All pupils are assessed by the Speech and Language (SALT) Team, who work closely with class teams to write and implement Communications Plans. The SALT Team are supported with technology by the ICT Team, as part of the scope of the wider Trans Disciplinary Team.

The overall aim is to assess for communication needs as part of any initial assessment, then support and promote the use of any aids within the school and home environment. Pupils will then be continually assessed throughout their time at TVS, trialling a range of different communication aids. Once a suitable aid is found, then support will be given to the family to get funding for a permanent device. Ongoing support and training will be provided by the SALT and ICT Teams to the families to promote the continued use of any aid during a pupil's time at TVS.

Students in their final years at TVs will also have fast track assessments with the SAT Team for communication aids, where appropriate, and funding sought so that communication can continue even after the student leaves TVS.

Following a review of the main communication software available, the ICT Team chose Sensory Software's *The Grid 2* software (soon to be superseded by *The Grid 3*) to support the needs of all pupils at TVS. Focusing on one software product means costs can be kept to a minimum for software updates and training, whilst maintaining continuity of using the same symbol set for all pupils across the school. The Grid software is used throughout the curriculum, for teaching and communication, with differentiation across the school to support the wide range of pupil needs at TVS. The SALT Team keep copies of any grids designed specifically for individuals and update them in conjunction with class teams.

The ICT Team hold lunchtime ICT Clubs for each Village, allowing pupils to have fun with technology.

There will be an ICT Day each year to cover areas that are not covered by embedded work. eSafety will also be addressed separately on Safer Internet Day in February.

Name of policy:	Information & communication technology policy
Effective from:	February 2015
Next review:	February 2017

Revision history

Date	Details	Author
Feb 2016	updated	Karen Calamaro
Nov 2015	Restyled	
Feb 2015		Karen Calamaro