TRURO SCHOOL

E-Safety Policy

A copy of this policy is published in the following area:
The school's website

Date created: October 2015 Reviewed: May 2018
Date for review: August 2018
Reviewed by Mark Vanstone, Director of Studies

A. Related Truro School Policies

Pupils will often have access to technologies that have both positive and negative potential. This policy aims to help ensure the school's expectations and safeguarding obligations are communicated and effective. It should be read along with the following policies:

- 9a Behaviour Policy – Rewards and Sanctions
- 7a Child Protection and Safeguarding Policy
- 10a Anti-bullying Policy
- Anti-racism Policy
- School Network and Internet Acceptable Use Policy
- Mobile Devices Policy
- Searching and Confiscation Policy
- Data Protection Policy

B. E-Safety Introduction

The school recognises that technology plays an important and positive role in everyone's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly. The general rule about digital technology is that it must not distract learning and must not be used to cause a disturbance or upset pupils, staff or members of the public. Digital technology must not be used in a way that is unsafe.

C. Aims and Duties

C1. Policy aims

The aims of this policy and other related policies are to ensure that:

- we safeguard the pupils in the real and virtual world

- pupils use digital technology in a responsible manner - the general rule is that digital technology must not distract learning and must not be used to cause a disturbance or upset pupils, staff or members of the public.
- pupils, staff and parents are educated to understand what cyberbullying is and what its consequences can be
- knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community
- we have effective measures to deal effectively with cases of cyberbullying
- we monitor the effectiveness of prevention measures.

C2. Legal duties and powers

- The school has a duty to protect all its members and provide a safe, healthy environment
- School staff may request a pupil to reveal a message or other mobile device content and may confiscate a mobile device.
- If they consider that a mobile device may contain evidence of bullying or a crime or the potential of a crime they may investigate the specific contents relating to that act; please refer to the Truro Search and Confiscation Policy for further guidance.
- Some cyberbullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997.

C3. Roles and responsibilities for online safety

E-Safety is part of the school's wider safeguarding strategy, and therefore part of child protection and pastoral care provision.

- One of our Deputies is the Designated Safeguarding Lead (DSL), the Director of Learning and Progression is the Deputy DSL.
- The management of pupil behaviour and the use of appropriate sanctions rests with the Deputy Head (Pastoral).
- Data Protection is the responsibility of the Director of Studies.
- Network security is the responsibility of the Network Manager who is the point of contact with the South West Grid for Learning, our internet service provider The Network Manager controls filter settings, maintains the password policies, maintains virus and spam checkers, maintains network access rights and is the one who is the first point of contact for the South West Grid for Learning (SWGfL) and police when there are queries from them.

C4. Technical provision and the safeguards used to filter and monitor inappropriate content and alert the school to safeguarding issues

- For our computer networking, we use Research Machines Community Connect 4, a complete school network management toolset designed specifically for education: https://www.rm.com/products/rm-community-connect
- For internet filtering, we use the SWGfL filtering system including RM SafetyNet Plus: http://swgfl.org.uk/products-services/schools-internet-service/SWGfL-Filtering
- The core SWGfL services are: Essential Safety

All traffic passed through SWGfL core network is checked against IWF CAIC list. Uniquely, SWGfL works with five Police forces and partners, enabling action on attempts to access illegal content.

C5. Essential Security

- Centralised enterprise-class Cisco firewalls
- Intrusion detection and prevention
- Market-leading Cisco IronPort solution for web / email security
- Service accredited to ISO27001 as well as other standards
- Filtering: the South West Grid for Learning comply with the Internet Watch Foundation which means that all illegal and criminally obscene content is automatically filtered in line the IWF legal requirements.
- RM SafetyNet Plus: a web filtering service designed specifically for educational establishments.
- Enables you to customise your local filtering and provides you with complete control over which websites, search engines and file extensions your users can access.

We can also choose to provide enhanced access for staff via 'Staff Proxy' ensuring staff are protected against illegal sites, but are able to access all other sites that are filtered for students. RM is a member of the Internet Watch Foundation and every day through their work with the IWF, they block millions of attempts to access web sites that they know to contain offensive material. These web sites include both unsuitable and illegal material that would otherwise have been accessed, either inadvertently or by intent.

YouTube for Schools™ is provided by YouTube and allows us to view educational videos from within school while filtering YouTube.com where there may be inappropriate content. It gives us the ability to access a broad set of educational videos on YouTube EDU and set up a specific playlist for our establishment.

C6. Monitoring by the network team

Use of the network is monitored by the Network Manager and his team, who regularly check workstation usage remotely and alert teaching staff when inappropriate activity takes place. This generally involves gaming, but can sometimes include pornography or inappropriate emailing. Network staff check a list of sites accessed from the school, which can lead to specific sites (such as VPNs and proxy bypasses) being blocked.

C7. Building resilience in pupils to through education and information

- All 1st Year pupils are introduced to the rights and responsibilities which relate to network usage and are made aware of the Network Acceptable Use Policy, which is also printed in planners and appears as a splash screen as pupils log in on CC4. There is an E-safety component to the first year PSHEE programme.
- All 3rd Year pupils study how to keep safe online as part of the OCR Functional Skills IT course in their externally examined course.
- Other year groups do not receive IT lessons, so E-safety training comes through the PSHEE programme or as one-off events organised by pastoral staff.

C8. Staff professional development

We have a Child Exploitation and Online Protection (CEOP) ambassador trained by the CEOP Centre. As part of the INSET programme, she has provided updates to staff. The Head of Boarding, an Assistant Housemaster, Heads of Year and the Head of Computing completed online training on E-Safety in Autumn 2015. The Designated Safeguarding Lead also provides updates at Staff Meetings.

C9. Educating parents in online safety
At the 1st Year Welcome Evening parents are introduced to E-Safety fundamentals by the Designated Safeguarding Lead.

C10. Management of personal data
The school is compliant with the statutory requirements as detailed in the Data Protection Act 1998 and is preparing for the General Data Protection Regulation to come into force on 25 May 2018; the eight principles of the Data Protection Act are found on the web site: http://www.legislation.gov.uk/ukpga/1998/29/schedule/1. These are being superseded by the six principles in Article 5 of the GDPR.

Also see the Appendix on Data Protection Principles and Truro School Data Protection Policy.

C11. Data protection (staff)
Data protection is the responsibility of all members of staff.

- Staff must not disclose to a third party personal data associated with another member of staff, a pupil or a pupil's family. When sending emails, staff should ensure the anonymity of addressees by making use of the BCC (blind carbon copy) functionality when addressing emails to groups of recipients outside the school, such as groups of parents.
- Staff must ensure that when they obtain personal data from the school or from a parent or pupil in the course of their work, they do not retain copies of personal data associated with another member of staff, a pupil or a pupil's family on their personal devices.
- Printed materials containing personal data should also be processed in accordance with the principles of the data protection act, including not putting printouts containing personal data into regular rubbish bins, recycling or reusing the paper for scrap. All such materials should be shredded before disposal.
- Staff must ensure that computing devices connected to school accounts are kept secure whilst in and out of school and report any loss of data, or connected electronic equipment to the Network Manager, or Director of Digital Strategy immediately.
- Staff must not store personal data or commercially sensitive information on personal cloud folders, unencrypted USB memory sticks or unencrypted external hard drives.
- OneDrive folders associated with school email addresses are held on secure servers in Europe, in compliance with Data Protection legislation. In this case, it is acceptable for staff to temporarily store digital copies of files containing limited personal data, such pupil names and pupil photographs, as mark books or lists, but these files should contain only necessary information and should be processed in accordance with the eight principles of the data protection act, so they must not be used for any purpose other than educational administration, they should kept up to date, should be kept in password-protected areas and should be removed when no longer needed, at the latest, at the end of the school year in which they were created. They may be shared with other staff who require access to the data, but must not be shared with pupils or parents, must not be passed on to other organisations, especially when these are outside the EU and the data must not be used for purposes other than educational administration.
- Sensitive personal data should not be stored by staff on any cloud-based service, USB sticks or external hard drives. Selected sensitive personal data may be made available to parents through the school portal. Responsibility for what is shown on the Portal lies with the SLT. The Director of Digital Strategy is responsible for ensuring that appropriate security is maintained on the Portal.

- In exceptional circumstances, permission may be given by the Director of Studies for sensitive personal data to be stored on a portable device, for example for use by the Designated Safeguarding Lead (DSL). In this case, data will be stored in an encrypted form, will be password protected, the device will be for the exclusive use of the member of staff and any loss of hardware or data will be immediately reported to the Network Manager or Director of Studies.
- Staff must not disclose personal data to third parties without authorisation from the Director of Studies.

D. Pupil Personal Safety

Pupils need to be aware that inconsiderate use of email and the internet may lead to disciplinary sanctions being applied. Reckless use of digital technology, particular in relation to social media and the internet, may jeopardise their personal safety either at school or outside school.

Pupils should:

1. Be aware that any person they communicate with online (eg via social media, chat rooms, etc.) may pretend to be someone else.
2. Never arrange a meeting in person with anyone they have only communicated with by computer, without parental approval.
3. Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, expressing extreme political or religious views designed to incite hatred, discriminatory, threatening, or which make the pupil feel uncomfortable or unsafe in any way. If such a message is encountered the pupil should report it to a teacher or the School Network Manager.
4. Remember that anything they read online may not be accurate.
5. Ignore offers that involve either financial transactions or personal meetings.
6. Not disclose any personal details, such as their home address or telephone number, across the Internet.

E. Child Protection

Pupils are reminded that it is a criminal offence to make indecent images or to download indecent images from the internet or to distribute indecent images through any network, email system or by mobile device.

Staff are also reminded that The Protection of Children Act 1978 prohibits at Section 1(1)(a) the "taking or making" of an indecent photograph or pseudo-photograph of a child. According to the Memorandum of Understanding between Crown Prosecution (CPS) and Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003:

> "Making includes the situation where a person downloads an image from the internet, or otherwise creates an electronic copy of a file containing such a photograph or pseudo-photograph. To be an offence such "making" must be a deliberate and intentional act, with the knowledge that the image made was, or was likely to be, an indecent photograph or pseudo-photograph of a child."

F. Confiscation and exploration of a digital device or data stored on the network

- Teachers can confiscate a mobile device if they suspect any activity which breaches school rules or the law.
- Members of the Senior Leadership Team may request the investigation of pupil data stored on the school network system or cloud if they suspect it breaches school rules or is illicit.
- Where the person searches an **electronic device** they may examine any data or files on the device if they think there is a good reason to do so. **Anyone searching an electronic device needs to have another adult present, partly to protect themselves from any allegations from the pupil. That person would usually be the pupil's tutor or another member of staff trusted by the pupil.** If inappropriate material is found on the device it should be passed to the Deputy Head or Designated Safeguarding Lead (DSL) who will retain it as evidence (of a criminal offence or a breach of school discipline). If necessary the Deputy Head or DSL will contact the police.
- If a member of staff finds a **pornographic image**, they **must not distribute it** but they will confiscate the device and give it to the Deputy Head as evidence for a necessary sanction. If it is extreme or child pornography it must be delivered to the DSL; the DSL will then arrange to contact the police as soon as reasonably practicable. Images found on a mobile phone or other electronic device should be shown to DSL as evidence for a serious sanction; they can then be deleted unless it is necessary to pass them to the police.

G. Preventing Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. Extremism can be defined as:

> Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.
>
> *Keeping Children Safe in Education* (September 2016)

There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media in particular has become a major factor in the radicalisation of young people. The school monitors internet use, in conjunction with the South West Grid for Learning (SWGfL), and if a child or young person has accessed or viewed extremist content, the Designated Safeguarding Lead (DSL) or Deputy DSL should be informed. They will report the website through www.direct.gov.uk/reportingonlineterrorism as well as informing the police, either 101 in a non-emergency or 999 in an emergency. Advice will be sought via the DfE dedicated telephone helpline (020 7340 7264) or email (counter-extremism@education.gsi.gov.uk

If staff have concerns that a pupil may be at risk of viewing extremist or terrorist material, or of becoming radicalised, they should raise these concerns with the DSL or Deputy DSL. A risk assessment will be undertaken and, if appropriate, help will be provided for the pupil through the government's Channel programme.

H. Cyberbullying

H1. What is Cyberbullying?

"Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others." http://www.cyberbullying.org/ a website written by by Bill Belsey.

Cyberbullying can involve Social Networking Sites, like Twitter, Facebook and Myspace, emails and mobile devices used for messages and digital cameras. In addition;

- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying
- It can also go further in that it can invade home/personal space and can involve a greater number of people
- It can take place across age groups and school staff and other adults can be targeted
- It can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'cyberstalking'; vilification/defamation; exclusion or peer rejection;
- Impersonation; unauthorised publication of private information or images ('happy-slapping'); and manipulation
- It can be an illegal act

H2. Preventing cyberbullying

- Staff will receive training in identifying cyberbullying and understanding their responsibilities in developing E-safety. The DSL may delegate this training to another member of the Senior Leadership Team (eg The Director of Staff Welfare and Co-curricular or Director of Digital Strategy), the Head of PSHEE or the IT department, as appropriate. In this training all staff will be helped to keep up to date with the nature of cyberbullying, how it can be identified, how it can be prevented and the technologies that pupils are using.
- Cyberbullying is a pastoral issue, which relates to pastoral care and child protection. The strategy for dealing with this rest with the Deputy Head who is the DSL. The technology is related to IT and digital technology and is dealt with by the Director of Digital Strategy issue.
- The delivery of PSHEE and 1st Year IT lessons are an important part of preventative strategy and will discuss keeping personal information safe and appropriate use of the internet.
- It is desirable that the pupils will be involved in a response to cyberbullying. They will have a voice through their tutors and the School Council.
- Pupils will be educated about cyberbullying through a variety of means: assemblies, conferences, Anti-bullying Week, projects (IT, PSHEE,), etc.

- Pupils will sign a Safe and Acceptable Use Policy before they are allowed to use school computer equipment and the internet in school and parents will be encouraged to discuss its contents with their children.
- Parents will be provided with information and advice on e-safety and cyberbullying via literature, talks, etc.
- Pupils and staff will be involved in evaluating and improving policies and procedures.

H3. Promoting the positive use of technology

We will:

- Make positive use of technology across the curriculum
- Use training opportunities to help staff develop their practice creatively and support pupils in safe and responsible use
- Ensure all staff and pupils understand the importance of password security and the need to log out of accounts

H4. Making reporting easier

- Ensure staff can recognise non-verbal signs and indications of cyberbullying with regular CP update training.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement
- Publicise to all members of the school community the ways in which cyberbullying can be reported
- Provide information for all students including reassurances about 'whistleblowing' and the appropriate way of informing appropriate staff or parents about incidents they have witnessed
- Provide information on external reporting routes e.g. mobile device company, internet service provider, Childline, CEOP or the NSA

H5. Evaluating the effectiveness of prevention measures

- Identify areas for improvement and incorporate pupil's ideas derived from talking to tutors and pupil voice through the School Council.
- Conduct an annual evaluation including a review of recorded cyberbullying incidents.
- It is also desirable to publicise evaluation findings; celebrate what works and what improvements are planned

H6. Responding to cyberbullying

Most cases of cyberbullying will be dealt with through the school's existing Anti-bullying Policy and this must remain the framework within which incidents of bullying are investigated. However, some features of cyberbullying differ from other forms of bullying and may prompt a particular response. The key differences are:

- impact: the scale and scope of cyberbullying can be greater than other forms of bullying;
- targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets;
- location: the 24/7 and anywhere nature of cyberbullying;
- anonymity: the person being bullied will not always know who is bullying them;
- intent: some pupils may not be aware that what they are doing is bullying;
- evidence: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence;

- it is possible that a member of staff may be a victim and these responses apply to them also.

See the Anti-Bullying Policy for details about investigating bullying allegations, support for the bullied, and working with the bully and applying sanctions.

I. Appendix: Data Protection Principles

I1. Data Protection Principles

There are eight Data Protection Principles in the Data Protection Act of 1998:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For the purposes of the Data Protection Act of 1998, we are registered with the Information Commissioner's Office. The point of contact in the school is the Director of Studies.

The General Data Protection Regulation applies from 25 May 2018, superseding the Data Protection Act of 1998, it has six principles:

1) Personal data shall be processed lawfully, fairly and in a transparent manner.
2) Personal data shall be collected for specified, explicit and legitimate purposes.
3) Personal data shall be adequate, relevant and limited to what is necessary.
4) Personal data shall be accurate and, where necessary, kept up to date.
5) Personal data shall be retained for only as long as necessary.
6) Personal data shall be processed in an appropriate manner to maintain security.

Under GDPR, there is an overarching requirement for the data controller to be able to demonstrate accountability. Truro School does not have a Data Protection Officer, but the Director of Studies will continue act as the point of contact for data protection issues.

I2. Definitions
There are some important definitions for words which have a specific meaning under the Data Protection Act.

Personal data means data which relate to a living individual (a Natural Person under GDPR) who can be identified:

(a) from those data;

or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data (Special Category Data under GDPR) means personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject;
(b) political opinions;
(c) religious beliefs or other beliefs of a similar nature;
(d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
(e) physical or mental health or condition;
(f) sexual life;
(g) the commission or alleged commission by that person of any offence;

or

(h) any proceedings for any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

Special category data is broadly similar to the concept of sensitive personal data under the 1998 Act. The requirement to identify a specific condition for processing this type of data is also very similar.

One change is that the GDPR includes genetic data and some biometric data in the definition. Another is that it does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

Data controller means:

- a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

A data controller must be a “person” recognised in law, that is to say:

- individuals;
- organisations; and
- other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.
Therefore, Truro School is the Data Controller.

J. Appendix: further information and contacts

- ChildNet International: Specialist resources for young people to raise awareness of online safety and how to protect themselves
- Information Sharing: advice for practitioners providing safeguarding services, DfE, March 2015
- Keeping Children Safe in Education, DfE, July 2015
- Prevent Duty Guidance for England and Wales, DfE, March 2015
- What To Do If You Are Worried A Child Is Being Abused, DfE, March 2015
- Working Together to Safeguard Children, DfE, March 2015
- The South West Safeguarding and Child Protection Procedures, http://www.swcpp.org.uk/
- Child Exploitation and Online Protection Centre (CEOP), http://www.ceop.police.uk/
- Think U Know: resources provided by Child Exploitation and Online Protection (CEOP) for children and young people, parents, carers and teachers; www.thinkuknow.co.uk
- Digizen: provides online safety information for educators, parents, carers and young people.
- Advice on Child Internet Safety 1.0: The UK Council for Child Internet Safety (UKCCIS) has produced universal guidelines for providers on keeping children safe online.
- Data Protection Act 1998, the eight principles are found on the web site http://www.legislation.gov.uk/ukpga/1998/29/schedule/1
- Information about the General Data Protection Regulation 2018 can be found on the Information Commissioner's web site, for example at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Research Machines Community Connect 4, a complete school network management toolset designed specifically for education. https://www.rm.com/products/rm-community-connect.
- The SWGfL filtering system including RM SafetyNet Plus http://swgfl.org.uk/products-services/schools-internet-service/SWGfL-Filtering