Online Safety Policy

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

Date created: October 2015
Reviewed: February 2021
Date for review: February 2022
Reviewed by Mark Vanstone, Director of Studies and Emma Ellison, Deputy Head Pastoral

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
- Searching and Confiscation Policy
- Data Protection Policy
- PSHEE policy and Schemes of Work
- Computing Schemes of Work

B. Online 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 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 from 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 from 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 online threats and what their consequences can be
- knowledge, policies and procedures are in place to prevent incidents of cyberbullying, child sexual exploitation, radicalisation and sexual predation in school or within the school community
- we have effective measures to deal effectively with cases of online threats
- 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
Online safety is part of the school's wider safeguarding strategy, and therefore part of child protection and pastoral care provision.

- The Governing Body is responsible for ensuring the staff undergo regular updated safeguarding training and all pupils are taught about online safety.
- The Deputy Head (Pastoral) is the Designated Safeguarding Lead (DSL), the Director of Co-Curricular and Head of Boarding are the Deputy DSL.
- The management of pupil behaviour and the use of appropriate sanctions rests with the Deputy Head (Pastoral) and Senior Pastoral Lead.
- Data Protection is the responsibility of the Business Director.
- 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 through our network security settings, ensuring staff are protected against illegal sites, but are able to access 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.

ClickView provides a video library for the school which can be used in lessons and accessed online by students. This allows us to view educational videos from within school without needing to access YouTube.com where there may be inappropriate content. It gives us the ability to access a broad set of educational videos 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 appears as a splash screen as pupils log in on CC4. There is an online safety component to the first year PSHEE programme.
- All 3rd Year pupils study how to keep safe online.
- Year groups above the 3rd Year do not receive IT lessons, so Online safety training comes through the PSHEE programme or as one-off events organised by pastoral staff. Tutor time and Head of Year assemblies are used to discuss key issues.
- All pupils are parents are given information which covers
content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults;
conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

3

C8. Staff professional development

As part of the INSET programme, staff have been updated concerning online-safety, data protection and how to report concerns to the Designated Safeguarding Lead. This forms part of the Level 2 single agency Child Protection training delivered to all staff at induction and updated every 3 years. Key members of the pastoral team completed online training on Online Safety in Spring 2018. The Designated Safeguarding Lead attends regular training on online safety and also provides updates at Staff Meetings/ Inset.

C9. Educating parents in online safety

At the 1st Year Welcome Evening parents are introduced to Online Safety fundamentals by the Designated Safeguarding Lead. Online safety is an integral part of pastoral parents' evenings throughout the school and there are frequent bulletin updates via email, as information is passed to the school, or issues arise.

C10. Management of personal data

The school is compliant with the statutory requirements of the General Data Protection Regulation (GDPR) which came into force on 25 May 2018 and the school is registered as a Data Controller with the Information Commissioner's Office. The six principles of the GDPR are as follows:

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 the GDPR, there is an overarching requirement for the data controller to be able to demonstrate accountability. The Business Director is the point of contact for data protection issues. For more information, please see the Truro School Data Protection Policy.

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, particularly 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. Do not disclose any personal details, such as their home address or telephone number, across the Internet.

E. Child Protection on Indecent Images

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. The local School Police Liaison Officer attends school regularly to give talks on Sexting and Online safety.

Further guidance of sexting can be found at Sexting in Schools and Colleges

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

Please see Searching and Confiscation Policy for details on dealing with inappropriate content.

G. 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 Snapchat, 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;

5

- 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 Online safety. The DSL may delegate this training to another member of the Senior Leadership Team, 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 whole school issue, which relates to pastoral care and child protection. The strategy for dealing with this rests with the Deputy Head Pastoral who is the DSL. The use of digital technology within the school is overseen by the Director of Studies, who also line manages the Network Manager.
- 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, the Anti-bullying Ambassadors 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 agree to 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.

H. Appendix: further information and contacts

Key Government Documents
- Keeping Children Safe in Education, DfE, September 2020
- Working Together to Safeguard Children, DfE, July 2018
- Information Sharing: advice for practitioners providing safeguarding services, DfE, July 2018
- Prevent Duty Guidance for England and Wales, DfE, April 2019
- Teaching Online Safety in Schools, DfE , June 2019

Useful websites
- ChildNet International : Specialist resources for young people to raise awareness of online safety and how to protect themselves including a section on cyberbullying
- 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/
- thinkuknow: resources provided by Child Exploitation and Online Protection (CEOP) for children and young people, parents, carers and teachers; www.thinkuknow.co.uk
- disrespectnobody.co.uk Home office advice on healthy relationships, including sexting and pornography

- [UK safer Internet centre](#) contains specialist helpline for uK schools and colleges
- [internet matters](#) and [parentzone](#) Help for parents on how to keep their children safe online
- [PSHE association](#) Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
- [educateagainsthate](#) Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
- [NSPCC](#) advice for schools and colleges
- [Net-aware](#) NSPCC advice for parents
- 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.
- 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