Online Safety Protocol

Date of Last Review:	1/11/2022	**Review Period**:	Annually
Date of Next Review:	1/11/2023	**Owner**:	Rachael Faulkner Deputy Headteacher

Introduction

The Trafalgar School at Downton takes its responsibilities for safeguarding extremely seriously. A growing part of this duty concerns safeguarding our students in a digital age. We aim to educate and inform our students to allow them to use the increasing amount of technology available to them safely, and without fear of harm.

Our protocol has been revised to incorporate the four Cs in KCSIE 2022:

1. **Content**
2. **Contact**
3. **Conduct**
4. **Commerce**

1. Content

The school plans its curriculum in Computing and PSHCE to give students the tools to protect themselves, when they are exposed to inappropriate content. In school, appropriate filtering is in place and the safeguarding team are alerted if there is an inappropriate search through the school portal RM Unify. If a student is found to be using school computing equipment this can result in a ban or their access being limited to only word processing products.

Through PSHCE, students are allowed a safe space to discuss and consider their response to topics such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism. This is also supported the pastoral theme of the week and tutor activities such as the Big Question.

We always mark Safer Internet Day with a series of activities in tutor times and lessons across the school.

Each year we have a week of anti-bullying assemblies with a focus on cyber – bullying. This is also written into our anti-bullying protocol. Students are clear about the reporting structures for cyber bullying incidents as per our bullying protocol

Students have regular updates during the year in assemblies as and when required – for example keeping safe with gaming, social media updates.

2. Contact

Our school filters and monitoring systems provide protection in school but we need to give our students the tools to use the digital world safely when they are in their homes and with their friends. Our 'Yondr' phone protocol was brought in to protect students in school from social pressure, mental health issues surrounding social media, and to give them time to enjoy talking and socialising with their friends. Through PSHCE, we give them an understanding of what

online grooming is and the different ways that advertising and peer pressure can affect the way they behave.

3. Conduct

We work with students and families to ensure they realise the severity of offences such as taking and sending nude pictures or sending them on to other students. We will always involve the police to record instances of this and the police support us in educating and discussing with students for early intervention as required. We also have a zero tolerance stance to online bullying and we recognising our responsibility, even out of school hours, to work with families to keep their children safe and to give them the information to do that. Regular updates are sent home by our Designated Safeguarding Lead (DSL) when there is a particular online risk to students. We often refer them to resources from external agencies such as the NSPCC who produce clear guidelines on a range of issues. Teaching our students to be appropriate users of digital technology is one of the greatest responsibilities in school today and we will use every avenue of support we can.

In addition, we also update staff with advice and guidance.

The changing nature of digital technology means that advice is only current for a small amount of time and we need to ensure that we are reactive and responsive to new concerns.

4. Commerce

During PSHE and Computing we teach students about the perils of online gambling, inappropriate advertising, phishing and scams. We regard it as extremely important to give our students the knowledge about how to avoid these fraudulent activities when they are using the Internet.

Hardware and software

The Trafalgar School at Downton uses a range of devices including PCs, laptops, and tablets. In order to safeguard students and in order to prevent the loss of personal data, we employ the following assistive technology:

Internet Filtering – We use software that prevents unauthorized access to illegal or inappropriate websites. Appropriate and inappropriate is determined by the age of the user and is reviewed in response to a change in requirements or legislation, whichever is sooner. The Network Manager and School Leadership Team are responsible for ensuring that the filtering is appropriate.

Email Filtering – Microsoft Exchange Online Protection is enabled on our Office365 Email Platform, which prevents any infected email being sent from or

received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Any personal device should not hold any personal data from the school. A remote desktop is provided for work from home. USBs, External Hard drives, Personal Laptops and Computers that are not owned by Trafalgar should not contain any personal data related to the school or its activities.

Passwords – All staff and students are unable to access any device without a unique username and password. Staff passwords will change every 45 days, or if there has been a compromise, whichever is sooner. This is the User's responsibility; a password protocol is enforced on behalf of the Trafalgar School at Downton.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives are scanned for viruses before use.

Safe use of Equipment and – Use of the Internet within the school is a privilege, not a right. Internet use will be granted to staff upon acceptance of the protocol and staff are required to indicate they accept the terms of the protocol each time they log-on to a computer.
email. Students are given their own email address and have acceptable usage protocols which they must follow.

Safeguarding concerns

Any concerns re inappropriate use of digital technology are referred to our DSL and dealt with in line with our safeguarding protocol. The CT network manager, in particular, alerts our DSL if there is inappropriate use of search engines or websites and the students are dealt with in a variety of ways. This may involve a ban from the network for a certain amount of time or contact with home or involvement of the PCSO/police or social care, depending on the severity of the issue. Each case is dealt with on an individual basis so that the student is aware of what they have done wrong, and how to approach a similar situation in the future. We look at how can educate rather than punish for the majority of cases.

This protocol should be read in conjunction with the following:

- The Trafalgar School Safeguarding and Child Protection Protocol
- The Trafalgar School Behaviour Protocol
- The Computing and PSHCE Curriculum Overviews
- The Pastoral Themes for the week and Big Questions
- The Network Agreement
- The Cybersecurity Awareness Agreement