TRURO HIGH SCHOOL
Where Girls Thrive

POLICY 32

ONLINE SAFETY AND MOBILE DEVICES POLICY INCLUDING REMOTE LEARNING

Policy reviewed by	Deputy Head, Health & Wellbeing
Governors' Committee	Education & Pastoral
Date reviewed	Michaelmas 2022
Next review date	Michaelmas 2024
Approval / Oversight	Oversight

TRURO HIGH SCHOOL

ONLINE SAFETY AND MOBILE DEVICES

1. Introduction

This policy applies to all pupils in the School, including those in EYFS.

Truro High School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. They allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of its commitment to learning and achievement, the School wants to ensure that the Internet and other digital technologies are used:

- To raise educational standards and promote pupil achievement;
- To develop the curriculum and make learning exciting and purposeful;
- To enable pupils to gain access to a wide span of knowledge and skills in a way that ensures their safety and security;
- To enhance and enrich their lives and understanding.

To enable this to happen, the School takes a whole-school approach to online safety, which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

Truro High School, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. The School recognises that ICT can allow all pupils increased access to the curriculum and other aspects related to learning.

Truro High School is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies safely. It is also committed to ensuring that all those who work with children and young people, as well as their parents/carers, are educated as to the risks that exist so that they can take an active part in safeguarding children.

The School's Designated Safeguarding Lead (DSL) and her deputies have a key role to play in overseeing the safety of pupils online. In this, they are supported by specialist teachers and technical staff, who have an important role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments.

The ICT Strategy Committee, chaired by the Bursar, considers online safety as part of its meetings, and discussions take place in other fora, such as the Welfare Team meetings, as appropriate.

The Network Manager is responsible for the security of the school network and for monitoring network traffic. The Head of Prep, Senior Deputy Head (DSL), Deputy Head, Health & Wellbeing (DDSL) and the Network Manager jointly monitor the appropriate use of the school network by pupils, staff and visitors through the Impero system (see below).

The Bursar is responsible for data protection at Truro High School and ensuring the School complies with legislation.

The Deputy Head, Health & Wellbeing and the Head of Prep, Senior Deputy Head are responsible for pupil behaviour, including behaviour on the school network and using digital technology. This includes

responsibility for monitoring and responding to cases of cyberbullying. See the School's Child Protection and Safeguarding including Child on Child Abuse policy and procedures and the Anti-Bullying policy.

All staff are ultimately responsible for monitoring pupils' use of the Internet, computers and mobile devices. Online safety regularly forms a part of safeguarding updates and training.

This policy should be read in conjunction with the following school policies:

- Child Protection and Safeguarding Policy including Child on Child Abuse
- Staff Code of Conduct
- Anti-Bullying Policy
- Behaviour Policy
- Conducting a Search Policy
- Data Protection Policy
- Prevent Duty Policy
- Acceptable Use Policy (see Appendix 1).

1.1 This policy has regard for:

- Keeping Children Safe in Education September 2022
- Teaching Online Safety in Schools – June 2019
- Education for a Connected World Framework
- *Sharing nudes and semi-nudes: Advice for education settings working with children and young people*. (UKCCIS) – December 2020
- National Crime Agency's Click CEOP reporting service
- Childline
- Internet Watch Foundation
- Harmful online challenges and online hoaxes – February 2021

2. Scope of Policy

The policy applies to:

- All pupils, including those in EYFS;
- All staff, including visiting staff, Governors and volunteers;
- All aspects of the School's facilities, where they are used by voluntary, statutory or community organisations at any time.

Truro High School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- A range of policies, including acceptable use policies that are frequently reviewed and updated;
- Information to parents which highlights safe practice for children and young people when using the Internet and other digital technologies;
- Adequate training for staff;
- A culture of responsibility shared by all when using the Internet and digital technologies;
- Education aimed at ensuring safe use of Internet and digital technologies;
- Monitoring of use and reporting procedures for abuse and misuse.

3. Filters and Monitoring

Working with Prosper and the Child Protection Company, web content at Truro High School is dynamically filtered via the School's Internet Service Provider (TAURUS), an internal firewall, a managed web filter portal and an internal proxy.

In addition, the School uses Impero Education Pro. Impero makes use of keyword detection and logs any use of words or phrases which are associated with a variety of topics, such as terrorism, bullying and self-harm. These detections are logged and fed back to the DSL. Impero was developed with the assistance of numerous expert bodies, including the Internet Watch Foundation (IWF), the Anti-Bullying Alliance, Beat and the UK Council for Child Internet Safety.

Prevent Duty

All UK schools must have due regard to the need to prevent people from being radicalised or drawn into terrorism. This duty is known as the Prevent Duty. Truro High School utilises Watchguard web content filtering to protect children from viewing inappropriate content on the Internet. Watchguard updates with common filtered websites from a central database updated by other Watchguard users around the globe to ensure that pupils are kept safe when browsing the Internet. Watchguard fully integrates with the Children's Internet Protection Act (CIPA) and IWF. Impero also alerts the School to the use of words and phrases on the school network associated with terrorism, extremism or radicalisation.

Third Party Use

Truro High School will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisations take an approach to their activities that sees the welfare of the child as paramount. To this end, it expects any organisation using the School's ICT or digital technologies to have appropriate policies and procedures aimed at safeguarding children and young people and for reporting concerns.

4. Policies and Procedures

The School understands that effective policies and procedures are the backbone to developing a whole-school approach to online safety. The School's policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils.

The School seeks to ensure that Internet and mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

The School expects all staff and pupils to use the Internet and mobile and digital technologies responsibly and strictly according to the conditions below (for the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies, e.g. mobile phone, including Bluetooth applications, PDAs, etc.). These expectations are also applicable to any voluntary, statutory and community organisations that make use of the School's ICT facilities and digital technologies.

Users must not:

- Visit Internet sites, or make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Indecent and/or inappropriate images;
    - Promoting discrimination of any kind;
    - Promoting racial or religious hatred;
    - Promoting illegal acts;
    - Promoting terrorism or extremist views, or designed to radicalise individuals;
    - Any other information which may be offensive to peers or colleagues, e.g. abusive images, sites which promote violence, gambling sites, etc.

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

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

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative);
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist or anti-religious material;
- Material connected with violence, extremism and/or bomb making;
- Material connected with illegal taking or promotion of drugs;
- Material connected with software piracy;
- Material connected with other criminal activity.

In addition, users must not:

- Use the school network for running a private business;
- Enter into any personal transaction that involves the school network in any way;
- Visit sites that might be defamatory or incur liability on the part of the School, or adversely impact on the image of the School;
- Upload, download, or otherwise transmit (make, produce or distribute), commercial software or any copyrighted materials belonging to third parties outside of the school network, or to the school network itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - Financial information;
    - Personal information;
    - Databases and the information contained therein;
    - Computer/network access codes;
    - Business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate;
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;
- Assist with unauthorised access to facilities or services accessible via the school network;
- Undertake activities with any of the following characteristics:
    - Wasting staff effort or networked resources, including time on end systems accessible via the school network and the effort of staff involved in support of those systems;
    - Corrupting or destroying other users' data;
    - Violating the privacy of other users;
    - Disrupting the work of other users;
    - Using the school network in a way that denies service to other users (e.g. deliberate or reckless overloading of access links or of switching equipment);
    - Continuing to use an item of networking software or hardware after the school network has requested that use cease because it is causing disruption to the correct functioning of the network;
    - Other misuse of the network, such as introduction of viruses;
- Use any mobile or digital technologies (e.g. 4G/5G) or mobile Internet services in any way to intimidate, threaten or cause harm to others;
- Use mobile or digital technologies to access inappropriate materials or encourage activities that are dangerous or illegal.

Where Prosper (as provider of Internet connectivity) and/or the Truro High School network become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the Police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

Pupils who fail to adhere to the School's policies and procedures can expect to face sanctions. These may include confiscation of a mobile device for a defined period; suspension of school network privileges for a defined period; school detention; or in serious cases, temporary or permanent exclusion. See the School's Rewards and Sanctions Policy.

Reporting abuse or misuse

Every user has a duty to report abuse or misuse of the school network or of mobile devices at school by any other user. The incident should be reported to either the Deputy Head, Health & Wellbeing (for the Senior School) or the Head of Prep, Senior Deputy Head (for the Prep School). If the abuse or misuse involves the Head of Prep, Senior Deputy Head or the Deputy Head, Health & Wellbeing, the matter should be reported to the Headmistress. If the abuse or misuse involves the Headmistress, it should be reported directly to the Chair of Governors.

There will be occasions when a user receives abusive or inappropriate communication, or accidentally accesses a website that contains abusive or inappropriate material. When such a situation occurs, the expectation of the School is that the user will report the incident immediately to either the Head of Prep, Senior Deputy Head or the Deputy Head, Health & Wellbeing.

The response of the School will be to take such incidents seriously and, where judged necessary, the DSL will refer details of an incident to the lead agencies involved in safeguarding children (MARU and CEOP).

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

Youth-Produced Sexual Imagery – Sharing nudes and semi-nudes

See the School's Child Protection and Safeguarding Policy including Child on Child Abuse and Anti-Bullying policies.

Searching an electronic device

See the School's Conducting a Search Policy.

5. Education and Training

The School recognises that the Internet and other digital technologies can:

- Transform learning;
- Help to improve outcomes for children and young people;
- Promote creativity;
- Create a more exciting and challenging classroom experience.

As part of achieving this, the School aims to provide an accessible system, with information and services online, which support personalised learning and choice. However, it realises that it will be necessary for pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

To this end, the School will:

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

The School's curriculum in Years 1-9 includes weekly Computing and IT lessons. The Senior School curriculum, in Years 7-9, leads to an in-house diploma. As part of these lessons, throughout the School, pupils are taught how to stay safe online. Particular attention is paid to helping pupils adjust their behaviours in order to reduce risks, including the safe use of electronic equipment and the Internet. The topic of cyber-bullying is addressed in both Computing and IT lessons and PSHE lessons. Online safety is also highlighted and discussed in assemblies. See also the School's Child Protection including child on child abuse and Anti-bullying policy.

Teaching about online safety -please see Teaching Online Safety in Schools – June 2019 for further detail

Underpinning knowledge and behaviours

Underpinning knowledge and behaviours include:

- **How to evaluate what they see online -** This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

- **How to recognise techniques used for persuasion** – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

- **Online behaviour** – This will enable pupils to understand what acceptable and unacceptable online behaviour look like. Schools should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

- **How to identify online risks** – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

- **How and when to seek support –** This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Schools can help pupils by:

- helping them to identify who trusted adults are,
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education September 2022); and
- helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Harms and risks

Understanding and applying the knowledge and behaviours above will provide pupils with a solid foundation to navigate the online world in an effective and safe way. However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils.

The tables referenced in Teaching Online Safety in Schools – June 2019 will help school staff understand some of the issues their pupils may be facing and where these could be covered within the curriculum. Schools should consider when it might be appropriate to cover these individual harms and risks. Any activity that does look at individual harms and risks should be considered in the broader context of providing the underpinning knowledge and behaviours, as set out in the previous section of this guidance.

Throughout the following sections we signpost to the Education for a Connected World Framework which includes age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives, including how to navigate online safely. This was developed by the UK Council for Internet Safety.

How to navigate the internet and manage information

This section covers various technical aspects of the internet that could leave pupils vulnerable if not understood.

Age specific advice on these potential harms and risks can be found in the following sections of the Education for a Connected World framework:

- Managing online information
- Copyright and ownership
- Privacy and Security

Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However, there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Schools should consider how they tailor their offer to ensure these pupils receive the information and support they need.

The following resources can help schools consider how best to support their most vulnerable pupils stay safe online:

- Vulnerable Children in a Digital World - Internet Matters
- Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group section
- STAR SEN Toolkit - Childnet

All pupils in the Senior School read and sign the Acceptable Use Policy annually (see Appendix 1 below). Teachers ensure pupils in the Prep School are aware of what is acceptable.

Staff also sign the Acceptable Use Policy as part of their induction and daily when logging in.

6. Monitoring

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and emails. The School recognises that in order to develop an effective whole school online safety approach there is a need to monitor patterns and trends of use inside school and outside school.

With regard to monitoring trends within the School and individual use by school staff and pupils, the School will audit the use of the Internet and email in order to ensure compliance with this policy. The monitoring

practices of the School are influenced by a range of issues and guidance notes and documents produced both nationally and regionally.

Pupils are expected to connect to the school network any mobile device which they bring to school, if they intend to use the device for anything other than making phone calls. Pupils are not permitted to use mobile devices in school using 4G or 5G.

The School is aware that pupils may choose to bypass the School's filtering systems by connecting their mobile devices to 4G and 5G. The School Rules make it clear that mobile phones should not be used during the school day (8.45am to 3.45pm), unless a teacher has given permission for the phone to be used for a specific task. Pupils may use other mobile devices or may use phones outside of these hours. (Sixth Form pupils are permitted to use mobile phones in the Sixth Form Centre during the school day.) Staff understand the need to monitor pupil use of mobile devices while in school and to ensure that these are not misused. When a member of staff finds a pupil using a mobile device against school policy or the School Rules, he/she will confiscate the item and report the matter to a member of SLT, who will investigate and determine whether a sanction should be imposed.

Boarding staff are aware of the opportunities in the boarding houses for pupils to bypass the School's filtering systems by connecting to 4G or 5G or by using a VPN, however most VPN services have been blocked by the school's firewall. They monitor use closely. Younger pupils are required to hand in their mobile devices at bedtime. If boarding staff discover a pupil misusing a mobile, the item is confiscated for a period of time. Other sanctions may also be applied.

7. Working in Partnership with Parents/Carers

The School is committed to working in partnership with parents/carers and understands the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

The School appreciates that there may be some parents/carers who are concerned about the use of the Internet, email and other digital technologies in the School. In such circumstances school staff will meet with parents/carers to discuss their concerns and agree upon a series of alternatives that will allow their daughter to fully access the curriculum, whilst remaining safe.

Where the School becomes aware of new technology or software which may pose a risk to pupils, it makes parents/carers aware of this and offers advice. This is often done via email updates. The School also runs events for parents on online safety from time to time.

8. National Online Safety Certified School:

The School is in the process of becoming a National Online Safety certified school. This will ensure that both staff and governors are fully trained but will also ensure that our parents/carers are fully informed and updated about online safety issues.

Appendix 1

TRURO HIGH SCHOOL
Girls First

Staff and Pupil ICT Acceptable Use Policy

Truro High School actively encourages employees to make use of ICT resources in a sensible and productive manner. There are limitations to how these resources may be used and Truro High School wishes to ensure that all employees understand the following conditions:

Acceptable Use

- Activities that include academic, administrative and research purposes;
- Use of ICT resources that does not violate any part of the Acceptable Use Policy;
- Remote administration of the network for authorised staff members;
- To gain access to school resources, files and software;
- To gain access to the school Management Information System (MIS), Pass/3Sys;
- To gain access to the Virtual Learning Environment (VLE).

Unacceptable Use

- Activities that could impact the fair, safe and productive use of the School's IT resources;
- Deliberate, unauthorised access to resources such as server files or pornographic Internet sites;
- Corrupting or destroying data deliberately;
- Deliberate, unauthorised access to resources such as proxy bypass sites or sites with inappropriate content
- Visiting chat sites, dating sites, gambling sites, torrent sites and any other websites which violate the School's filtering policy, online safety policy or the Internet Watch Foundation guidelines;
- Deliberate overloading of the network in a way that denies access to other users;
- Plugging a personal mobile device into any Ethernet ports outside of the Rashleigh or Dalvenie Houses;
- Unplug any school electrical equipment from its socket;
- Introducing viruses, spyware of trojans to the school network;
- Ex-employees attempting to access school resources;
- Using credentials other than your own to access school resources remotely.

Reason for the Policy

To provide a set of Terms and Conditions for users of the School's ICT resources and remote access services that restrict the ways in which this provision is used. It is common practice for users to agree to an Acceptable Use Policy before they are granted access to various IT resources. This is to protect both the School and the user.

Who is Affected by This Policy

This policy applies to all individuals who use school ICT resources and remotely access ICT resources owned by Truro High School. These individuals will include all staff members, students, and individuals given guest access on behalf of the School.

Misuse

Users who do not take these precautions could be subject to:

- Written or verbal warning;
- Suspension of remote access privileges;
- Suspension of the user's account;
- Termination of the user's account;
- Legal action.

Computer Use Policy

1. The mailbox, home directory and other storage space allocated to me on the school network servers and workstations remain the property of the School, including all the material contained within them, which must be used solely and exclusively for the purposes of furthering and promoting my education.

2. I do not have the right to store, download from the Internet or use any material of a violent, profane, insulting, obscene or racist nature or any material which if inadvertently or deliberately shown to other parties may cause offence.

3. I understand that I must not use the school network or school equipment to access material connected with terrorism or extremism, and I must not use the school network or school equipment to radicalise others.

4. I may not use any storage media to store materials as described in 2 or 3, and I understand that the Network Manager has the right to inspect any suspect media and confiscate it if found to contain such material.

5. I understand that the Network Manager and that person only, has the ability, and reserves the right, to inspect any mailboxes or home directories suspected of holding material of a violent, racist or obscene nature. I understand that any such material found will be removed and copied for use as evidence for taking severe action by the Headmistress and Governors.

6. I understand that I am not allowed to attempt to breach network security by attempting to gain unauthorised access either to the hard drives of the workstations or unauthorised areas of the server.

7. I understand that I am not allowed to log on in another person's name with or without their presence or consent.

8. I understand that I am not allowed to disclose my password to anyone else or give permission to another person to log on in my name.

9. I understand that any use of school-owned ICT resources is actively monitored and logged. Such records can be required, by law, if the need arises.

10. I understand that if I do not return a valid contract then I will not be entitled to a user's account or email.

11. I understand that the network administrators can remotely log into any school-owned device, without user consent, for troubleshooting and maintenance purposes.

Internet Access Policy

1. Network administrators will monitor all Internet access by staff members and pupils.

2. I understand that I will be subject to a certain level of filtering that is deemed appropriate for the School and will report any websites that I think may be deemed inappropriate for pupils.

3. I understand that pornographic sites, chat sites, dating sites, gambling sites, torrent sites and any other websites that violate the Truro High School filtering policy, online safety policy or the Internet Watch Foundation guidelines are strictly prohibited and must be reported immediately.

4. Network administrators will filter content and impose time restrictions where necessary.

Email Use Policy

1. Email must be used with discretion.

2. I understand that it is a violation to forge email or email signatures in any way.

3. I understand email is to be used strictly for business or academic purposes.

4. The distribution of chain email is a serious misuse of school resources and users will have their accounts disabled for participating in this activity.

5. I fully understand the dangers of email attachments and spam email and will report any concerns to the ICT Department.

Mobile Devices Policy

1. I understand that mobile devices, of any kind, should not be used in a manner that will prove disruptive to the normal routine of the School. Devices should be switched to silent unless it is being used as a learning tool in the classroom.

2. I understand, unless permission has been granted, that it is forbidden to take images (photographs or videos) in the school environment or store school files and folders on a mobile device. If I need access to these files and folders then I will use remote access.

3. Staff members are strictly prohibited from passing on their personal phone details to pupils and for connecting with pupils via social media.

4. I understand I am fully responsible for maintaining an anti-virus programme on my mobile device.

5. School-owned mobile phones given out to staff must be taken good care of and staff must take all reasonable precautions to ensure that the device is not damaged, lost or stolen. Any issues must be reported immediately.

6. School-owned mobile phones given out to staff are subject to regular monitoring of itemised monthly bills.

7. By using the school Wi-Fi, I agree to all terms and conditions within the Internet Access Policy.

8. Personal devices with access to school email should be password protected.

Remote Access Policy

1. I understand that I will be responsible for using strong passwords. Weak passwords are a simple way for an attacker to exploit a user's log in and legitimately roam the school network. Passwords should be at least eight characters long, include numbers and symbols, a mixture of uppercase and lowercase characters, and changed regularly. Never share your passwords.

2. I understand that I am responsible for implementing anti-virus software (e.g. Kaspersky or Norton) on the device connecting to the school's remote server. The anti-virus software must be running in real time with fully updated virus definitions.

3. I understand that I am responsible for maintaining vendor updates on my home operating system. Vendor updates are readily available from Microsoft and Apple and will help remediate security exposures in your operating system. There is usually an automatic update feature that will download and install at set times.

4. I understand that I am responsible for ensuring the built-in firewall of my device is enabled at all times when using remote access.

5. As a user, I agree to protect all sensitive/privileged/personal data and guard against inadvertent disclosure.

6. I understand that I must limit computer usage to myself when using remote access. When I am logged in remotely and not using my computer, I must ensure the computer is locked to prevent unauthorised access.

7. I am fully aware that I will be held accountable for all activities logged against my credentials. This includes any kind of misuse and illegal activity.

8. I have fully read and understood the Acceptable Use Policy and agree to abide by all terms and conditions stated.

9. I agree to abide by Truro High School policies and procedures. I also agree to abide by laws and legislations such as the Data Protection Act 1998.

Print Policy

1. All users will be given a termly allocation of print credits which will be reviewed on an on-going basis.

2. Users who exceed their allocated print credit must contact the Network Manager who will decide, based on prior print history, to either increase the print credit or seek payment in order to reactivate print credits.

3. I understand that my ability to print will be withdrawn if there is evidence of misuse. This can include, but is not limited to:
    a. Wasting resources e.g. printing multiple copies, printing documents with dark backgrounds, printing web pages;
    b. Printing of anything deemed 'offensive';
    c. Printing documents for personal use.

4. I understand that my print usage is subject to constant monitoring and reporting that will be assessed at regular intervals.

Monitoring

Internet usage is actively monitored on a daily basis. The School records details such as identity of user, sites visited, date, time and frequency. If inappropriate Internet usage is detected, then the perpetrator will face sanctions.

School staff members have the right to inspect any suspect media and confiscate it if we suspect material of a violent, racist or obscene nature deemed inappropriate for student use.

Staff members also reserve the right, to inspect any mailboxes or home directories suspected of holding inappropriate material. I understand that any such material found will be removed and copied for use as evidence for taking severe action with the Headmistress.

Contact Information

If you have any questions regarding this policy please direct your queries to the SLT or the ICT Department.

Name: .....

Signature: ..... Date:.....

Appendix 2 – Remote Learning Policy

Truro High School Remote Learning Policy

1. Background

This policy is to ensure the ongoing education of Truro High School pupils under the unusual circumstances of the forced school closure during Covid-19. This policy will also future-proof against closures that could happen at any time: due to illness or epidemic, extreme weather, power-loss, etc. It also covers the ongoing education of pupils who cannot attend their lessons in school for a period of time, but who do wish to continue with their education. This would, for example, include pupils recuperating from operations.

2. Remote Learning Lead

The Deputy Head, Health & Wellbeing in the Senior School and the Head of Prep, Senior Deputy Head in the Prep School are responsible for formulating and overseeing Truro High School's Remote Learning Policy. Any questions about the operation of this policy, or any concerns about the viability of any part of this policy, should be addressed to the Deputy Head, Health & Wellbeing or Head of Prep, Senior Deputy Head in the first instance.

3. Preparing for Remote Learning

We would expect that many of the steps below would already be in place with most staff within Truro High School. We would expect there to be future benefits to putting these steps into place for all teaching staff.

Truro High School will be proactive in ensuring that:

- Staff have access to Microsoft Teams for their classes, and that these are set up
- Pupils within classes have access to the relevant Microsoft Team
- Pupils will receive Teams refresher sessions (and specific Teams Meetings instruction) in IT lessons in Years 3-9 and during tutor periods for the rest of the school
- Staff are familiar with the main functions of Microsoft Teams
- Staff have the ability to host a Teams Meeting (video and/or audio) with their classes either from their classrooms or from home
- Parents and pupils are made aware in advance of the arrangements in place for the continuity of education

Truro High School should ensure that staff are supported in the development of the above framework by:

- Using staff meetings or setting aside professional development time. Truro High School's network manager has audited the settings in Teams and communicated this with staff during an INSET. He has also circulated all resources and training.
- Ensuring that staff have access to a suitable device in their classroom or, in the event of closure, that staff have suitable technology at home and if not, supply them with a device during the closure period.

4. Guidelines for staff during remote learning

Guidelines for staff:

- Only use your school-registered accounts, never personal ones.
- Only use Microsoft Teams for online lessons.

- Participate in lessons from a safe and appropriate place with no bedrooms or inappropriate objects/information visible. You can blur the background on Teams.
- Please ensure that you are wearing appropriate clothing at all times.
- Language must be professional and appropriate, including any family members in the background.
- Record all lessons so that they can be reviewed later if necessary or in line with safeguarding monitoring measures below.
- Begin each lesson by reminding pupils that the lesson is recorded and they may switch off their camera and/or microphone if they wish. Pupils should also be reminded to blur their background and ensure the door remains open.
- Make sure you remind girls to hang up first, before you, to ensure that live streaming is still not in use at the end of the lesson.
- Keep a log of all online interactions with pupils - what, when, with whom and any concerns of difficulties.
- Alert the Deputy Head, Health & Wellbeing or Head of Prep, Senior Deputy Head at the end of the school day if there are girls who are not attending lessons. The Deputy Head, Health & Wellbeing/ Head of Prep, Senior Deputy Head/SENCO will follow up any absences, particularly for our vulnerable students with SEND and CP needs.
- Prior to establishing a one to one arrangement above and beyond assisting a pupil within a whole class context, a member of teaching SLT should be informed and parental consent sought. E.g. one to one LAMDA or Learning Support lessons.
- For safeguarding monitoring, Deb Freeman should be added as a member to all Senior Teams and Katie Hinks to all Prep Teams so lessons may be joined by a member of SLT at any time.
- If you have any safeguarding concerns, please follow the school's CP and Safeguarding procedure and alert the DSL or DDSL's without delay. This includes any neutral notifications regarding your own behaviour or experiences online.
- Please remember that you have signed an Acceptable User Policy and ensure that you remind all pupils of appropriate online behaviour. Senior pupils should be reminded that they too have signed the policy. The rules are the same during remote learning.
- Inform the Deputy Head, Health & Wellbeing or Head of Prep, Senior Deputy Head if you are unwell or unable to teach online, ideally providing work that can be assigned through Teams. If possible, alert girls through Teams that you are unable to attend the lesson and assign the appropriate work yourself.

5. Guidelines for pupils during remote learning

- Only use your school-registered account (…@trurohigh.co.uk), never personal ones.
- Only use Microsoft Teams for online lessons.
- Participate in lessons from a safe and appropriate place with no bedrooms or inappropriate objects/information visible. If you do need to work from a desk in your bedroom, please ask us for help to blur your background on Teams.
- Ensure the door to the room you are working in is open so adults at home are aware of the lesson taking place online. Parents of young pupils may wish to be present for longer periods.
- Please ensure that you are wearing appropriate clothing at all times.
- Language must be professional and appropriate, including any family members in the background.
- Make sure that you hang up at the end of the lesson.
- All lessons are recorded by the teacher for safeguarding reasons and can be reviewed if necessary. Pupils must never record a lesson.

- Switch off your camera and/or microphone if you do not wish to be identifiable on the recording.
- Teachers will alert the Deputy Head, Health & Wellbeing or Head of Prep, Senior Deputy Head if you are absent and she will follow this up.
- If anything happens online that makes you feel uncomfortable, contact your Form Tutor or the Deputy Head, Health & Wellbeing/Head of Prep, Senior Deputy Head.
- All pupils have been taught how to behave safely and respectfully online and the rules are the same when learning remotely. Senior pupils, please remember that you have signed an Acceptable Users Policy.
- Please ensure that any chat and communication online is respectful and kind and follows our Child on Child Abuse and Anti-Bullying Policy.
- If there is any concern over behaviour, you will be removed from Teams and the Deputy Head, Health & Wellbeing/Head of Prep, Senior Deputy Head/Director of Teaching and Learning will contact home.

6. Monitoring

- A member of SLT must be added to all Teams.
- Learning walks, where a member of SLT may 'drop in', will continue as they normally would in school. If a full lesson needs to be audited for any reason, the teacher will be informed that the recording will be reviewed.