Tuition, Medical and Behaviour Support Service

E-Safety Policy

Adopted:	October 2025
Next Review:	September 2026
Governing Committee:	6 November 2025
Responsibility:	Matthew Brown & Dan McEntee

Contents

Introduction **3**
Responsibilities **4**
Personal Development, Behaviour and Welfare Working Party **4**
Internet use and Acceptable Use Policies (AUPs) **4**
The Prevent duty **5**
Filtering and Monitoring **6**
Photographs and Video **6**
Photos and videos taken by parents/carers **6**
Mobile phones and other devices **7**
Generative Artificial Intelligence (AI) **7**
Cyber-bullying **8**
Use of e-mails **9**
Security and passwords **9**
Data storage **9**
Reporting **10**
Infringements and sanctions **11**
Primary Students 11
Secondary Students 12
Staff 13
Social networking **14**
Pupils 14
Staff 14
Staff communication **14**
Education **15**
Pupils 15
Staff 17
Parents and the wider community **18**
Appendices **19**
Appendix 1 **20**
Acceptable Use Agreement KS1 20
Acceptable Use Agreement KS2 21
Acceptable Use Agreement KS3 and KS4 22
Staff Acceptable Use Policy 23
Internet Safety Awareness for Hospital Provision pupils 24
Appendix 2 **25**
Parental Agreement – E-Safety 25
Appendix 3 **27**
Consent for images of pupils being used 27
Appendix 4 **29**
E-Safety Induction for New Staff **29**

Introduction

Information Communication Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites
Apps
Artificial intelligence
Assistive Technology
E-mail, Instant Messaging and chat rooms
Social Media, including Facebook and Twitter
Mobile/ Smart phones with text, video and/or web functionality
Other mobile devices including tablets and gaming devices
Online Games
Learning Platforms and Virtual Learning Environments
Blogs and Wikis, Podcasting
Video sharing, Downloading
On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Tuition, Medical and Behaviour Support Service, we understand the responsibility to educate our pupils on e-safety Issues; as categorised within Keeping Children Safe in Education (KCSiE) into four areas of risk; Content, Contact, Conduct and Commerce. Please see KCSiE document (September 2025) Part 2: The Management of Safeguarding, for more information. Aspects of this are also referred to in our Safeguarding Policy, Behaviour Policy and Safeguarding Policy. TMBSS has a zero tolerance policy towards Child on Child abuse.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. Through the TMBSS Cyber Response plan, The Service aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulations (GDPR). Please see the TMBSS GDPR Policy and Cyber Response Plan for more details.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the service (such as PCs, laptops, mobile devices, whiteboards, digital video equipment, etc.). This also includes technologies owned by pupils and staff, but brought onto service premises (such as laptops, mobile phones and other mobile devices).

Responsibilities

The member of SLT team responsible for Safeguarding is	**James Pearson**
The governor responsible for e-safety is	**Steve Lunt**
The e-safety co-ordinator for Secondary is	**Dan McEntee**
The e-safety co-ordinator for Primary is	**Matthew Brown**

The secondary e-safety co-ordinator is responsible for e-safety as part of the Personal Development, Behaviour and Welfare Working Party (PDBW Working Party). Both the primary and secondary e-safety co-ordinators are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the college community. They may also be required to provide guidance to parents/carers. In each centre there are 2-3 Designated Safeguarding Leads, alongside the Senior Designated Safeguarding Lead.

Personal Development, Behaviour and Welfare Working Party

A member of the SLT chairs the service PDBW Working Party with responsibility for Safeguarding. It meets once per half term and will invite a representative of SLT, and a range of teaching staff. The ICT Working Party meets half-termly to discuss and action any outcomes from the PDBW Working Party.

Internet use and Acceptable Use Policies (AUPs)

All members of Staff will receive a copy of the Acceptable Use Policy (AUP) (Appendix 1) via email. In addition, from September 2022, staff have been required to sign in acknowledgment that they have read and understood it. Staff who do not sign will be given a printed copy of the document by a member of the SLT. The SLT member will sign to say that the staff member has been given the document.

Visitors who require internet access are given the password for TMBSS Guest Wi-Fi, which requires them upon log on, to manually acknowledge that they are agreeing to abide by the Acceptable Use Policy.

Temporary members of staff, including Supply Teachers are required to acknowledge the Staff AUP and complete the e-safety induction before being given a username and password.

In Primary, the AUP will be explained during the pupils' induction to Centre by their class teacher before they can use any ICT equipment. This is part of the baseline paperwork completed by class teachers.

A signed copy will be kept in Harlescott Education Centre. A copy will also be sent home to Parents. Any child who does not complete the AUP, will not be allowed to use ICT equipment at TMBSS.

In Secondary, the AUP will form part of the pupil’s home visit and baseline paperwork prior to entering the Service in secondary, a copy of the pupil AUP (Appendix 1) will be sent to parents with a Parental Agreement (Appendix 2). A signed copy will be kept in the allocated secondary centre.

In Hospital provisions, an AUP is signed by parents when patients are using a TMBSS laptop. This document is kept in the patient's file by the Hospital Educational Coordinators.

AUPs will be reviewed annually. Student & Parent AUPs will be stored within each Centre in case of breaches of the e-safety policy.

The Prevent duty

The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The Prevent duty requires all education providers ‘to help prevent the risk of people becoming susceptible to an extremist ideology.

The Prevent duty means that all staff have a duty to be vigilant. This means where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

Learners are at risk of accessing inappropriate and harmful extremist content online. There is a rapid proliferation of terrorist content online and the internet has become the preferred avenue for those searching for terrorist propaganda. This could include downloading or sharing terrorist material, which could be a criminal offence.

Some children are at greater risk of harm than others, both online and offline and the risks and vulnerabilities are listed in greater detail within the Prevent Policy which also gives guidance and actions for concerns.

As Designated Safeguarding Lead, James Pearson will oversee Prevent on behalf of TMBSS. The Service doesn’t need consent to share information about a pupil who might be susceptible to radicalisation.

More generally, TMBSS play an important role to equip children and young people within the Service to stay safe online, both in school and outside. In Primary, internet safety is taught as part of the ICT Curriculum and forms part of the RSE curriculum. In addition to this, termly assemblies are delivered addressing safe use of the internet. In Secondary, internet safety will be integral to the Service’s ICT curriculum and is embedded in PSHE. General advice and resources on internet safety are linked from the e-safety page on the Service website.

Further information on the Prevent procedures can be found in the TMBSS Prevent policy.

Filtering and Monitoring

TMBSS ensures that suitable internet filtering is in place. As of September 2023, all centres are equipped with Fortigate Firewalls. Internet usage and reporting is provided using Fastvue. IPads are used across the service and these are managed using Apple School Manager, with additional security through JamF. As part of their safeguarding and online safety training, staff understand their expectations, roles and responsibilities around filtering and monitoring systems. As per Keeping Children Safe in Education 2025, the Senior Designated Safeguarding Lead along with the Chair of Governors, have overall responsibility for making sure that the standards in terms of filtering and monitoring are met.

Photographs and Video

Technology is used to record children's learning in a variety of ways, including photographs and videos. This is kept secure by only saving the information onto TMBSS's secured shared areas. These shared areas can only be accessed by staff whilst they are at TMBSS centres, or with a limited number of enabled TMBSS devices outside of the centre. In TMBSS, iPads are also used to record children's learning. As mentioned, these are managed using Apple School Manager and JamF. Photos and other documents are regularly deleted from the iPad's which are stored securely in storage lockers.

It is important that consent from parents is gained if videos or photos of pupils are going to be used. If photos/videos are to be used online then names of pupils should not be linked to photographs unless permission has been granted.

Staff must be fully aware of the consent form responses from parents when considering use of images.

The Consent form used is in Appendix 3.

Staff should always use a Service device to capture images and should never use their personal devices.

Photos taken by the Service are subject to the GDPR. Please see the TMBSS GDPR policy for more information.

Photos and videos taken by parents/carers

In Primary it is requested that no photos/videos are taken at Service Open Days. In Secondary, parents and carers are permitted to take photos/videos of their own children in Service events. They are requested not to share photos/videos from Service events on social networking sites if other pupils appear in the background.

The Parental Agreement concerning AUPs includes a paragraph concerning posting photos on social networking sites (Appendix 2).

Photos for personal use such as those taken by parents/carers are not subject to the GDPR. Please see the TMBSS GDPR policy for more information.

Mobile phones and other devices

Appropriate use of mobile phones is essential at TMBSS. Practitioners can use their personal mobile phones during their break times or in cases of emergency or for medical reasons. During working hours, they must be kept out of the reach of children in an area accessible only to staff. All staff are aware of their duty to follow this procedure, and to challenge anyone not adhering to it.

Most of our Primary students do not have their own mobile device. Any that do are required to hand it in for safe storage during their session in Centre.

Secondary pupils are expected to hand in their phones for safe storage before entering a centre. They are handed back to pupils upon leaving the centre. There is a separate policy on the use of Mobile Phones which covers unacceptable use in more detail and the sanctions for not following the policy.

Through induction, staff and volunteers are made aware of our Acceptable Use Policy both at home and in the workplace. If any staff or volunteers breach this policy, then we may take disciplinary action which may result in a referral to the Disclosure and Barring Service.

TMBSS subscribes to a number of web-based software solutions which allow staff to work more flexibly. Some of these include, Microsoft Outlook Webmail, Microsoft One Drive and CPOMS. There are a number of implications around the use of these on personal devices due to the sensitive nature of some personal data. Staff are advised not to save passwords for any of these websites on a personal device. This is of particular importance when the device is used by other people. Staff are also advised not to install a smartphone or tablet application for any of these services on a personal device. Some staff (SLT, DSL and members of ICT Working Party) are required to use 2 factor authentication Apps on their personal devices in order to increase the level of security for access to sensitive information. These security apps do not access any sensitive information on the devices which they are installed.

Generative Artificial Intelligence (AI)

Generative AI is one type of AI. It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources.

Staff are encouraged to follow the guidance on the guidance paper Generative artificial intelligence (AI) in education (2025) which states;

“Teachers, leaders and staff must use their professional judgement when using these tools. Any content produced requires critical judgement to check for appropriateness and accuracy. The quality and content of any final documents remains the responsibility of the professional who produced it and the organisation they belong to, regardless of the tools or resources used.

Generative AI tools can make certain written tasks quicker and easier, but it cannot replace the judgement and deep subject knowledge of a human expert.
The education sector should:

- make the most of the opportunities that technology provides
- use technology safely and effectively to deliver excellent education that prepares pupils and students to contribute to society and the future workplace
- be aware of the limitations and risks of this technology"

We believe that AI should be used to enhance, not replace, learning. Staff promote the use of AI as a helper, not a thief.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the TMBSS behaviour policy.)

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Service will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with all students.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the Service will follow the processes set out in the Child-on-Child Abuse Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Use of e-mails

Staff should only use e-mail addresses that have been issued by the service for work. Staff are advised not to install smartphone or tablet applications to access work email on a personal device. In emergencies, users should log in and out of their web browser, without saving the password on the device. Members of SLT and ICT Working Party are required to use 2-factor authentication to access their emails.

All secondary students will be allocated an email when they start in the service. This email is for use in ICT lessons. Students will use their email for MS Teams meetings, if necessary and for college applications if needed. These emails are not to be used for any purpose other than school.

Within the hospital teaching environment, students will be using either their own personal emails or that of their registered school. With short term patients/pupils teachers follow hospital guidelines and policies, however longer term patients/pupils and parents sign an adapted version of the Acceptable Use Policy (Appendix 1).

Security and passwords

Passwords for the TMBSS network for students and teachers are required to be changed every three months. The system will inform users when the password is to be changed. Passwords for email accounts are synchronised to these passwords. Staff should never share passwords. Staff should never let pupils use a staff logon. There are occasions when secondary students may need access that requires a teacher logon. In these circumstances, they should never be without strict supervision by a member of staff. Staff must always ‘lock’ a PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and allow a PC to be ‘locked’).

In TMBSS Primary, pupils are never left unsupervised with a digital device. Laptops are logged on, using individual student usernames by staff. Students have an iPad designated for their use.

Within the hospital teaching environment, teachers use a mix of devices that belong either to that hospital or TMBSS. All devices are encrypted as they use public Wi-fi.

All users should be aware that the ICT system is filtered and monitored. In the main service buildings, this is completed by TMBSS filtering service. These are in line with the KCSiE document (September 2025) and consider the need for reasonable restrictions which allow content regarding online teaching and safeguarding. This is overseen by the E-Safety Governor.

Data storage

In accordance with the GDPR Policy, encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Staff, pupils or governors who store sensitive information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our

Acceptable Use Policy). For more information regarding what is defined as sensitive (personal) information please see the GDPR policy.

Reporting

All breaches of the e-safety policy by pupils need to be recorded on CPOMS as an e-safety Incident. These should alert members of the ICT Working Party.

Incidents which may lead to child protection issues need to be followed up with a Designated Lead immediately – it is their responsibility to decide on appropriate action not the member of staff.

Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying, as defined in the Child-on-Child Abuse Policy and in the Cyberbullying section of this policy). This should also be verbally followed up with a member of SLT on the same day.

Allegations involving staff should be reported directly to the Executive Head. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained where possible.

Both the Primary and Secondary curriculum cover "Keeping safe online". This includes how to stay safe, use the internet responsibly and report a problem. There is also an e-safety page on the Service website, where students and parents/carers can access more information and report any concerns.

- Notification reports of all TMBSS computer users are compiled via Fastvue and they are shared and reviewed by ICT and Safeguarding leads.

- The impact of the e-safety policy and practice is monitored through the review/audit of filtering reports, CPOMS reports, surveys of staff, students/pupils and parents/carers.

- The records are reviewed/audited and reported to:
  - the SLT
  - Governors
  - Shropshire Local Authority (where necessary)
  - Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

- The e-safety and ICT policies are reviewed annually to reflect the latest guidance.

- The ICT subject development plan indicates any planned action based on the above.

If pupils are being asked to learn online at home, for example because of the coronavirus pandemic, TMBSS will follow the advice from the DfE on safeguarding and remote education. Please also refer to the TMBSS Remote Learning Policy for further information.

With regard to e-safety matters (Child on Child abuse etc.) that occur via social media or online outside of education, parents would be advised to contact the Police directly to make a complaint if TMBSS were made aware.

Infringements and sanctions

Whenever a student or staff member infringes the e-safety Policy, the final decision on the level of sanction will be at the discretion of the SLT. In all instances of infringement evidence should be secured and preserved where possible.
Here are some examples:

Primary Students

In TMBSS Primary, students should never be left unsupervised with a digital device. It is the responsibility of the adult working with that pupil to ensure the Acceptable Use Policy is adhered to. Any infringement should be reported to the Class Teacher, e-safety co-ordinator and Assistant Head. Depending on the nature of the infringement, a sanction will be applied immediately. Usually this will be the removal of ICT privileges for a set amount of time. Serious and repeated infringements may be logged on CPOMS as an e-safety incident.

If there are Safeguarding implications, the information must be shared with a Designated Safeguarding Lead and logged on CPOMS.

Secondary Students

Level 1 infringements

- Visiting unappropriated website. Use of unauthorised instant messaging / social networking sites
- Sharing password with other students and using other accounts

Sanctions: *Conversation with Centre Manager, incident logged on daily report. To also include specific sanctions from the TMBSS Mobile Phone Policy.*

Level 2 infringements

- Continued use of unappropriated websites after being warned
- Unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Downloading or upload anything to the internet
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

Sanction: *Referred to e-safety Coordinator, removal of Internet access rights for a period of time set by Centre Manager/e-safety co-ordinator, logged on CPOMS as an e-safety incident and contact with parent/carer. To also include specific sanctions from the TMBSS Mobile Phone Policy.*

Level 3 infringements

- Deliberately corrupting or destroying someone’s data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

Sanction: *Referred to e-safety Coordinator, SLT and Designated Lead (Safeguarding), removal of Internet access rights for a period of time set by Centre Manager/e-safety co-ordinator, logged on CPOMS as an e-safety incident and contact with parent/carer. To also include specific sanctions from the TMBSS Mobile Phone Policy.*

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the GDPR. Please see the TMBSS GDPR policy for more information.
- Bringing the service name into disrepute

Sanction: *Referred SLT, Executive Head, Designated Lead (Safeguarding) and e-safety coordinator, refer to Community Police Officer, LA e-safety officer and SSCB, logged on CPOMS as an e-safety/Child Protection incident and contact with parent/carer. To also include specific sanctions from the TMBSS Mobile Phone Policy.*

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of the Service if they are related to the Service.

Staff

Staff are required to follow the Service's Code of Conduct. Sections 10, 11, 12 and 13 of this document cover communication and social interaction with children using technology.

Level 1 infringements (Misconduct)

- Use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. in school time using service equipment.
- Misuse of data security, e.g. allowing students using laptop on staff account, writing down password.
- Breaching copyright or license e.g. installing unlicensed software on network
- Not reporting any e-safety incidents correctly
- Using mobile phone in front of students, except for medical reasons
- Personal information about students is saved incorrectly

Sanction: *Referred to Executive Head. Warning given.*

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any service / Council computer hardware or software;
- Any deliberate attempt to breach GDPR or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the GDPR. Please see the TMBSS GDPR policy for more information.
- Bringing the Service name into disrepute.

Sanction: *Referred to H / Governors and follow service disciplinary procedures; report to LA Personnel/ Human resources, report to Police. For further information please refer to the TMBSS Safeguarding and Child Protection Policy.*

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

It is likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Social networking

Pupils

Pupils are not permitted to use social networking sites within the Service. These sites are blocked on all TMBSS devices. As part of the Curriculum, “Keeping safe online” is taught and includes how to use the internet responsibly and report a problem. Regular assemblies are held in Primary to promote e-safety. Safer Internet Day is promoted annually throughout the Service. Unacceptable use of social networking sites is also covered in our Mobile Phone Policy and Safeguarding Policy.

Staff

It is recognised that social networking sites have a major role to play in today’s society. Social networking sites are blocked on all TMBSS devices. However, staff must be aware of the following:

- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of service events.
- Staff must not use social networking sites via personal devices within lesson times
- Staff need to use social networking in a way that does not conflict with the TDA Core Standards or TMBSS Staff Code of Conduct. (Section 10, 11 and 12)
- Staff should review and adjust their privacy settings regularly to give them the appropriate level of privacy.

Staff communication

Staff should only communicate with pupils and parents through official channels. These channels include:

- Face to face
- A printed letter on service letter headed paper
- Service telephone system
- Service provided mobile phone
- Service e-mail system and Microsoft Teams

The following are excluded from the official channels:

- Social networking sites
- Gaming sites
- Chatrooms
- Personal mobile phones
- Personal e-mail addresses
- Personal video conferencing solutions (e.g. Zoom)

Education

Pupils

In the Keeping Children Safe in Education document (2024) it states Safeguarding, including online safety should be taught as part of a broad and balanced curriculum. In the National Curriculum, it states that students need to learn about the following areas of online safety as part of the curriculum.

In Key Stage 1, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

In the Teaching online Safety in School Guidance Document (2019) it gives three section of advice in more detail of the potential Harms or Risks of online behaviour and the curriculum area this could be covered in. The sections are How to navigate the internet and manage information, How to stay safe online, and wellbeing (pg9 – 23)

The PSHE curriculum also includes the following areas in terms of E-Safety:

- **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; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and financial scams.

The safe and responsible use of social media and the internet will also be covered in other subjects where relevant.

The RSHE curriculum also includes the following areas in terms of E-Safety:

Primary:

Online relationships:
Students should know

- that people sometimes behave differently online, including by pretending to be someone they are not.
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.

Online and media:
Students should know

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- what to do and where to get support to report material or manage issues online.
- the impact of viewing harmful content.
- that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- how information and data is generated, collected, shared and used online.

Internet safety and harms:
Students should know

- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- where and how to report concerns and get support with issues online.

Secondary:

Internet safety and harms:
Pupils should know:

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online.
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

In Primary, internet safety is taught as part of the ICT Curriculum and forms part of the RSHE curriculum. TMBSS Primary will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite external visitors to talk to pupils about this, as recommended in Teaching Online Safety in School Guidance Document (2019). In Secondary, internet safety will be integral to the Service's ICT curriculum and is embedded in PSHE. TMBSS is committed to developing a whole school approach to teaching online safety. We aim to do that by

- Creating a culture that incorporates the principles of online safety across all elements of school life,
- Proactively engaging staff, pupils and parents/carers,
- Reviewing and maintaining the online safety principles,
- Embedding the online safety principles

TMBSS has a higher percentage of students vulnerable to harm online. As described in the Teaching Online Safety in School Guidance Document (2019) "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." This means that, as with other areas of the curriculum, the teaching of online safety is personalised to each student's needs. To find resource for supporting vulnerable refer to page 24 of Teaching Online Safety in School Guidance Document (2019).

Safer Internet Day is promoted annually throughout the Service. Also as a part of the PSHE KS4 Curriculum the students, in the summer 1 term, complete the AQA unit award 112259 understanding the risk and benefits of social media posting

Staff

- An audit of e-safety training needs is carried out regularly and is addressed
- A planned programme of formal e-safety training is delivered to all staff in the form of 'Bitesize' sessions that are delivered during staff meetings and updated annually in response to the e-safety survey. This includes the NCSC Cyber Security Training for School Staff.
- E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
- All staff have an up to date awareness of e-safety matters, the current service e-safety policy and practices and child protection / safeguarding procedures

- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the Service e-safety policy and Acceptable Use Policy
- The culture of the Service ensures that staff support each other in sharing knowledge and good practice about e-safety and has a zero-tolerance approach to Child on child abuse
- The Service takes every opportunity to research and understand good practice that is taking place in other schools
- Governors will undertake e-safety training as part of their safeguarding training.

Parents and the wider community

Parents/carers are kept informed of e-safety via the website and newsletter. An annual parental survey is conducted to allow parents to raise concerns regarding online safety and identify gaps in knowledge. These are then addressed through the e-safety action plan to reinforce the importance of children being safe online.

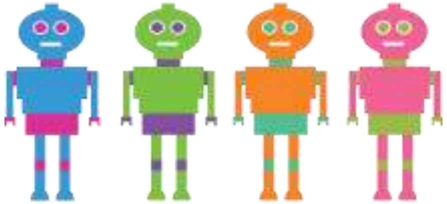
Appendices

Appendix 1

Acceptable Use Agreement KS1

At School:

I know anything I do on the computers or iPads may be seen by someone else.	
I will not load photos of myself onto the computer or take them with the iPad.	
I will not play games (unless told to by my teacher) during lesson time.	
I will only open pages which my teacher says are OK.	
I will talk to my teacher before using anything on the internet.	
I will look after the laptops and iPads. I will always hold them carefully, especially when moving about.	



At Home:

I will only play online with people I know in real life.	
I will tell a grown up if anything makes me feel scared or uncomfortable.	
I will make sure any messages I send are polite.	
I will show an adult if I get a nasty message.	
I will not reply to any nasty message or anything which makes me feel uncomfortable.	
I will not tell people about myself online (I will not tell them my name, anything about my family and home, phone numbers or pets' names).	
I will never agree to meet a stranger.	

I have discussed these rules with _______________ and they understand what is expected from them and what to do when there is an issue.

Signed (Teacher):…………………………………………………..

Date…………………………

Signed (Pupil):………………………………………………

Date…………………………

Signed (Parent/Carer):…………………………………………….

Date…………………………

Acceptable Use Agreement KS2

At School:

I know anything I do on the computers or iPads may be seen by someone else.	
I will not load photos of myself onto the computer or take them with the iPad.	
I will not play games (unless told to by my teacher) during lesson time.	
I will only open pages and Apps which my teacher says are OK.	
I will talk to my teacher before using anything on the internet.	
I will look after the laptops and iPads. I will always hold them carefully, especially when moving about.	
I will keep any logins and passwords secret.	
I will only edit or delete my own files. I will not look at, or change, other people's files.	

At Home:

I know that you can only use some websites and social networks if you are old enough.	
I know that you can only play some games if you are old enough.	
I know it is not healthy to spend a long time on a tablet or computer. It can affect your sleep and mood.	
I will not load photos of myself onto the internet. I know that people can take a copy or see things that are put on the internet, even if I delete them.	
I will only play games, message or speak to people that I know, or a grown-up has approved. I know it is safer to play games online with people I know in real life.	
I will never agree to meet someone I have played with online that I don't know.	
I will not tell people I play with online my name, anything about my family and home, phone numbers or pets.	
I will tell an adult if I receive a message that upsets me or people talk online about things that upset me.	
I will tell an adult if I see an advert or video that upsets me.	
The messages I send, chats I have and information I upload, will always be polite and sensible.	
I will not reply to any nasty message or anything which makes me feel uncomfortable. I will always show an adult.	
I will not open an attachment, or download a file, unless I know and trust the person who has sent it.	

I have discussed these rules with _______________ and they understand what is expected from them and what to do when there is an issue.

Signed
(Teacher):…………………………………………

Date…………………………

Signed
(Pupil):……………………………………………

Date…………………………

Signed
(Parent/Carer):………………………………

Date…………………………

Acceptable Use Agreement KS3 and KS4

At School:

I will set a strong password and not share it with other students	
I will only visit sites which are appropriate	
I will report unsuitable content or activities to a member of staff	
I will follow the copyright law and not copy other peoples work	
I will only communicate with people online who have been approved by my teachers	
I will not use memory sticks without permission	
I will not download or upload anything on to the internet	
I will hand my phone in when I get to centre	
I will treat myself and other with respect when online	
I will only play games on the computer when given permission	
I will always log off my computer when I have finished using it	
I will only use school email for contacting people as part of a learning activity	
I will not try and download anything from the internet	

I know:

I Know that anything I do online may be monitored	
I know once I shared anything online it is out of my control and could be used be by others	
I am aware of the CEOP report button and I know how and when to use it	

CEOP REPORT
ceop.police.uk

I have discussed these rules with ________________ and they understand what is expected from them and what to do when there is an issue.

Signed (Staff):...
Date.............................

Signed (Pupil):.......................................
Date.........................

Signed (Parent/Carer):.............................
Date.............................

Staff Acceptable Use Policy

I have read the TMBSS Acceptable Use Policy. I understand that this policy is guidance and is written to raise staff awareness and provide protection in their roles. I understand what is expected from me and what to do if there is an issue. I understand by logging onto the TMBSS system, I acknowledge my understanding of the TMBSS Acceptable Use Policy.

I understand the need to

Follow all policies regarding ICT, Computing, E-safety, Safeguarding and GDPR. I understand that it is my responsibility to read and be aware of these policies.
Set a strong password and not share it with anyone else. Use MFA(Microsoft Authenticator) to access accounts securely when off site.
Only use my service email account for work.
Not have any friendships/contacts with students on social media platforms including, but not limited to; Facebook, Snapchat, TikTok, Instagram and personal email accounts.
Follow the copyright law and not copy other people's work.
Ensure all personal information about students is saved to the TMBSS Sharepoint, or an encrypted device until a time that it can be uploaded to the appropriate secure area.
Ensure any personal information that is digitally communicated or transported with or to other professionals is through an encrypted email or website e.g. ePEP, CPOMS, DfE.
Only take and post photos of students using equipment belonging to the Service, when appropriate consent has been given by parents/carers or themselves.
Look after all ICT equipment used by me or students under my supervision and report any damage or misuse to the Assistant Head, Centre Manager and ICT co-ordinator immediately.
Report E-safety incidents via CPOMS as outlined in the E-safety policy.
Not use my personal mobile phone for personal use in front of students, unless in an emergency or for medical reasons.
Ensure my personal mobile phone is stored securely and out of the reach of students.
Ensure that any private social networking sites, blogs, etc that I create or contribute to do not compromise my professional role.
Promote the positive use of Technology, Digital Literacy and Online Safety.
Ensure that my use of Service printing facilities is work-related and appropriate.

I understand that

Anything I do online may be monitored and could be used to compromise my professional role.
Once I have shared anything online it is out of my control and could be used by others.

Tuition, Medical and Behaviour Support Service (TMBSS)

Internet Safety Awareness for Hospital Provision pupils

Dear Parents / Carers,

It is vital that children are able to keep themselves and others safe and use the internet responsibly. We understand that as teachers, we have an important role in raising pupil's awareness of the potential dangers of using the internet and helping them develop strategies to avoid these risks and keep safe online. As a TMBSS Hospital Teacher in Shropshire, it is helpful if we have written agreement about internet safety relating to your child whilst being educated in hospital.

Many thanks,
Ward Teacher

Be Responsible

I will….

- Use TMBSS electronic devices as directed by my teacher.
- Use only my own accounts .
- Follow International copyright laws.

Be Respectful

I will….

- Communicate online in a respectful manner.
- Be careful to treat equipment with care.
- Respect the work and privacy of others.

Be Safe

I will….

- Keep my password and login information private.
- Tell and adult if I read something on the internet that makes me feel uncomfortable.
- Refrain from sharing my personal information on the internet.

Please could you read the items below and circle your response then sign and insert your child's name and date.

As the parent/ legal guardian I grant permission for my son /daughter to access the Internet and other ICT facilities. I understand the Tuition Medical and Behaviour Support Service rules for responsible ICT use as outlined in the Acceptable Use Policy (AUP) on the Hospital section of the TMBSS website. I understand that TMBSS cannot be held responsible for the nature & content of materials accessed through the Internet & mobile technologies. I understand that TMBSS will take all reasonable precautions to keep pupils safe and to prevent pupils from accessing inappropriate materials. I will support the service's approach to E-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of others.	**Yes or No**

Signed: (Parent / Carer) Name of Pupil: Date:

Appendix 2

Tuition, Medical and Behaviour Support Service

Parental Agreement – E-Safety

Pupil name(s): ………………………………………………………………………

Education Centre: ……………………………………………………………

Parent's signature:…………………………………………… **Date:**…………………

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, service Email and other ICT facilities at TMBSS. I know that my daughter or son has signed a form to confirm that they will keep to the service's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the service cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the service will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the service can check my child's computer files, and the Internet sites they visit. I also know that the service may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the service by promoting safe use of the Internet and digital technology at home and will inform the service if I have any concerns over my child's e-safety.

I am aware that the service permits parents/carers to take photographs and videos of their own children in service events and that the service requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the service's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the service community.

Tuition, Medical and Behaviour Support Service

Shropshire Council
TMBSS
Central Office Administration
Sundorne Education Centre
218 Sundorne Road

Our Ref: SM/MB

Dear Parent/Carer,

In order for my child to have permission to access to use the Internet and other ICT facilities at TMBSS they have signed the attached the Acceptable Use Policy (AUP). We would be grateful if you could go through the attached document and discuss the guidelines at home as well. Once you have done so, please sign and return the attached form.
Until we receive this completed form, your child will not be able to use the ICT facilities at TMBSS.

Yours sincerely

Matthew Brown

Matthew Brown
ICT Co-ordinator
Harlescott Education Centre

01743 460252
admin@tmbss-shropshire.org.uk

Appendix 3

Tuition, Medical and Behaviour Support Service

Shropshire Council
TMBSS
Central Office
Administration
Sundorne Education
Centre
218 Sundorne Road

Our Ref: KR/LB

Dear Parent/Carer

Consent for images of pupils being used

Increasingly, pupils at the Education Centres are being involved in projects which may involve their photograph or video image being taken. It is possible that images will be displayed around the Centres, used for publicity purposes, and may appear in the local press or even on television.

Guidance from Shropshire Council recommends that written parental consent is obtained before a pupil’s image can be used outside of the Centre.

I would, therefore, be grateful if you could complete and return the attached sheet to me at your earliest convenience.

Yours sincerely

Greg Portman

Greg Portman
Head of Service

01743 368189
admin@tmbss-shropshire.org.uk

Consent form for taking and using photos

Child’s name: ____

Date: ____

Dear parent/carer

At Tuition, Medical and Behaviour Support Service, we occasionally photograph or video pupils as evidence of pupils participation in a range of educational activities. We use these photos in the school’s newsletter, on the school’s website and on display boards around school.

We would like your consent to take images of your child, and use them in the ways described above. If you’re not happy for us to do this, that’s no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take images of my child. □

I am happy for images of my child to be used on the school website. □

I am happy for images of my child to be used in the school newsletter. □

I am happy for images of my child to be used in internal displays. □

I am **NOT** happy for the school to take or use photos of my child. □

I am **NOT** happy for the school to take or use videos of my child. □

If you change your mind at any time, you can let us know by emailing admin@tmbss-shropshire.org.uk, calling the school on 01743 368189 or just popping into the school office.

If you have any other questions, please get in touch.

Parent or carer’s signature: ____

Date: ____

Appendix 4

E-Safety Induction for New Staff

	DATE COMPLETED	SIGNED BY STAFF MEMBER TO INDICATE READ AND UNDERSTOOD
E-SAFETY POLICY		
ACCEPTABLE USE POLICY		
BITESIZE E-SAFETY INCIDENT		
BITESIZE E-SAFETY PHOTOGRAPHY		
BITESIZE MEMORY STICK (ENCRYPT OR NOT ENCRYPT)		
BITESIZE HOW TO LOCK A COMPUTER		
BITESIZE CYBERBULLYING		
BITESIZE HOW TO BLOCK OR UNBLOCK A WEBSITE		
NCSC CYBERSECURITY FOR SCHOOLS		PRINT CERTIFICATE
BITESIZE KEEPING SAFE ON VARIOUS SOCIAL MEDIA		

SIGNED BY MEMBER OF ICT WORKING PARTY:

…………………………………………………………….

NAME: …………………………………………………………….

DATE: …………………………………………………………….

For all ICT support and queries please:

Email: ict.support@mmat.co.uk

This will create a ticket on our service desk and ensure any queries do not get missed.

Telephone: 01691 664488

Remote Support: https://get.teamviewer.com/mmatict

Your Support Technician: James Ritch

(Please direct support emails to the above address)

Head of IT Outreach: Mike Foden

(mike.foden@mmat.co.uk)

Marches Academy IT Director: Ian Hopwood

(ian.hopwood@mmat.co.uk)