Tuition, Medical and Behaviour Support Service

E-Safety Policy

Adopted:	May 2019
Next Review:	May 2020
Governing Committee:	2 May 2019
Responsibility:	Sian McGrory & Matthew Brown

Contents **Page**

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
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 three areas of risk; Content, Contact and Conduct. Please see KCSiE document Annexe C, for more information. Aspects of this are also referred to in our Peer on Peer Abuse Policy, Behaviour Policy and Safeguarding Policy.

Schools hold personal also 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. TMBSS 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 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	**Dr Charles Woodford**
The e-safety co-ordinator for Secondary is	**Sian McGrory**
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.

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 (AUP's)

All members of the Staff will sign an Acceptable Use Policy (AUP) that is appropriate to their age and role (Appendix 1).

In Primary each teacher will explain the AUP to new pupils before they can use any ICT equipment.

A signed copy will be kept in Harlescott Education Centre. A copy will then be sent home for Parents to sign and return with the covering letter (Appendix 2). 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.

AUP's will be reviewed annually. Student & Parent AUP's will be stored within each Centre in case of breaches of the e-safety policy, staff AUPs will be stored centrally in the admin office at Sundorne.

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 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

TMBSS ensure that suitable internet filtering is in place. 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.

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 and secure cloud services e.g. Gridmaker. These shared areas can only be accessed by staff whilst they are at TMBSS centres, or with a limited number of enabled TMBSS devices. In TMBSS, Primary iPads are also used to record children's learning. These are managed by "Mini Mac" server. Photos and other documents are regularly deleted from the iPad's which are stored securely.

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 AUP's 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. 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 allowed to keep their phones on them but they must be switched off and put away during lessons. They are directed on how to use their devices appropriately within school and reminded that they should not charge their devices, take photographs or videos whilst in TMBSS centres. They cannot connect to TMBSS Wi-Fi, but if their device has mobile access to the internet, they will be able to get online. 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, Gridmaker, CPOMS and iTrack. 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.

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 email on a personal device. If necessary, users should log in and out of their web browser, without saving the password on the device.

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 six weeks. The system will inform users when the password is to be changed. Staff are advised to change their email password at the same time. 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. PCs are usually logged on, using student usernames by staff.

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. Within the Primary hubs, teachers use devices that belong to TMBSS, but connect to that school's internet, therefore is filtered by the filtering service provided by that school. These are in line with the KCSiE document, and takes into account the need for reasonable restrictions which allow content with regard to online teaching and safeguarding.

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. A weekly notification report is shared and reviewed by ICT and Safeguarding leads, which identifies breaches of the TMBSS Acceptable Use Policy.

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 Peer on Peer Abuse Policy) should be also verbally followed up with a member of SLT on the same day.

Allegations involving staff should be reported directly to the Head of Service. 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.

With regard to e-safety matters (Peer on peer abuse etc.) that occur via social media or online outside of Centres, parents are to be advised to contact the Police directly to make a complaint.

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:

a) Primary Students

In TMBSS Primary, pupils 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 Centre Manager. 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.

b) Secondary Students

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

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 non-educational sites during lessons after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of File sharing software
- 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, Head of Service, 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.

(c)Staff

Staff are required to follow the Service's Code of Conduct. Sections 10, 11 and 12 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. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

Sanction - Head of Service. 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 Head of Service / 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 Peer on Peer Abuse 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 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

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. Skype)

Education

Pupils

In the Keeping Children Safe in Education document (2018) it states Safeguarding, including online safety should be taught as part of a broad and balanced curriculum. In the National Curriculum, it states that pupils need to learn about the following areas of online safety as part of the curriculum.
In Key Stage 1, pupils 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

Pupils 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, pupils 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

Pupils 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
-

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.

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

TMBSS Primary will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Safer Internet Day is promoted annually throughout the Service.

Staff

- An audit of e-safety training needs is carried out regularly and is addressed
- A planned programme of formal e-safety training is made available to all 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
- The Service takes every opportunity to research and understand good practice that is taking place in other schools
- Governors are offered the opportunity to undertake training.

Parents and the wider community

Parents/carers are kept informed of e-safety via the website and newsletter.

Monitoring and reporting

- A weekly notification report of all TMBSS computer users is shared and reviewed by ICT and Safeguarding leads, which identifies breaches of the TMBSS Acceptable Use Policy.

- 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)

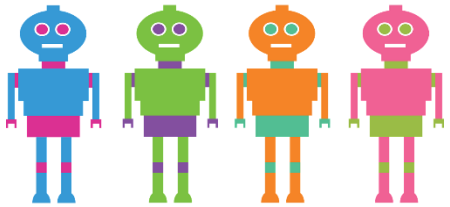
- The ICT subject development plan indicates any planned action based on the above.

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	

Mobile Phones:

I will only use in centre when given permission by staff	
I will only send and post appropriate messages or images	
I will not take photos or film in centre	
If I receive inappropriate messages I will share them with a trusted adult	
I will, if asked, turn my mobile phone off	
I will only charge my phone in centre with permission	
I will keep my phone away during lessons	

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	

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.....

Tuition, Medical and Behaviour Support Service

Parental Consent for images of pupil's being used in Hospital Provision.

Princess Royal Hospital

Dear Parents/Carers,

From time to time we like to take photographs of the children as mementoes of their time spent at Princess Royal Hospital. It is possible that photographs will be displayed around the Paediatric Ward or used for publicity purposes to illustrate and promote the work of Princess Royal Hospital. Photos may also appear on the hospital website, TMBSS Educational website or in the local press /television.

We now have to ask that written parental consent is obtained before a pupil's image can be used. I would, therefore, be grateful if you could complete the form below.

Many Thanks

Hospital Teacher, Princess Royal Hospital.

Pupil's name:_____

* Please delete where appropriate.
* I give / do not give my permission for his / her image and name to be used in publicity material /press releases issued by PRH or TMBSS Education Service.
* I give / do not give my permission for his / her image and name to be posted on the TMBSS Education website.
* I give / do not give my permission for his / her image to appear on television.

Signed :_____(Parent/Carer)

Acceptable Use Policy

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. 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 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. I understand that the service can check my child's computer files, and the Internet sites they visit.

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.

Signed: _____

Date: _____

Tuition, Medical and Behaviour Support Service

Acceptable Use Policy for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the service network security
- follow all service policies in relation to ICT computing, Safeguarding, GDPR and Conduct. It is my responsibility to be aware of the expectations regarding these policies.
- respect the copyright and intellectual property rights of others
- only use work email accounts for any service correspondence
- ensure emails containing personal information are encrypted
- students are referred to by initials only in all emails
- ensure only pupils with consent for images are taken or published as appropriate.
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site, unless permission has been given.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety co-ordinator
- promote any supplied e-safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/Service policies, e.g. gambling
  - do anything which exposes others to danger
- post any other information which may be offensive to others
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files containing personal data on a portable device or cloud-based storage system without permission from the Head of Service or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that GDPR policy requires me to keep any information I see regarding staff or pupils which is held within the service's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the service and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used as evidence.

Name: _____

Signed: _____

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
Centre Manager – Harlescott Education Centre

01743 368190
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 368190
admin@tmbss-shropshire.org.uk

Parental consent for images of pupils to be used

Pupil's name _____

Education Centre _____

*** I give/do not give** my permission for his/her image and name to be used in publicity material/press releases issued by the Education Centre.

*** I give/do not give** my permission for his/her image and name to be posted on the Centre's website

*** I give/do not give** my permission for his/her image to appear on television.

***Please delete where inapplicable.**

Signed _____ (parent/carer)

Date _____

Please return to:

Greg Portman,
Head of Service
TMBSS Central Office Administration,
Sundorne Education Centre,
218 Sundorne Road,
Shrewsbury,
SY1 4RG