Truro and Penwith
Academy Trust

Blackwater
Community Primary School

Blackwater School Technology Policy

To include Use of Images of children, Mobile Phone, Acceptable Use and to be read in conjunction with TPAT's Social Media Policy (2020)

Sept 2024 – Sept 2025

Safeguarding

Blackwater School is committed to safeguarding and promoting the welfare of all children. We expect all our team members to share this commitment.

1. Purpose of Policy

This policy sets out how Blackwater School will ensure the safety and welfare of children in our care when using technology.

This policy is designed to ensure that potential issues involving technology can be clearly identified and addressed, ensuring the benefits of technology can continue.

All adults within the school must accept the policy before using technology on school premises or using technology for school use out of school.

Introduction

In Blackwater School we believe that the internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides children with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

We use a school website (www.blackwatercornwall.sch.uk). It is used by children, staff and families as a central source of information, as well as celebrating the achievements of the school. The ethos, vision and values of Blackwater School are identified in the appearance and content of the website.

We use social media to reach out to parents/carers in a forum in which we know many are active participants. The school operates a Facebook Page named 'Blackwater Community Primary School.' The administrators will only use the Facebook page to signpost to the school's website and to promote the school.

Schools need and welcome publicity. Children's photographs add colour, life and interest to articles promoting school activities and initiatives. Making use of photographs for publicity materials and to promote the school in the press can increase child motivation and staff morale and help parents/carers and the local community identify and celebrate the school's achievements. However, photographs must be used in a responsible way.

In May 2004, section 45 of the Sex Offences Act 2003 amended Section 1 of the Protection of Children Act 1978 by raising the age of a 'child' from 16 to 18. This means it is now an offence to 'take, make, allow taking, distributing, showing, possessing with intent to distribute, or advertise indecent photos or pseudo photographs of children under the age of 18. Blackwater School recognises the need to respect children's and parents/carers' rights of privacy and is aware of potential safeguarding issues.

The policy has been drawn up by the staff of the school under the leadership of the Headteacher & Computing Leader. It has been approved by Governors and is available for parents/carers to see.
The policy and its implementation will be reviewed annually. The Computing Leader will monitor the effectiveness of the policy, particularly in the light of new developments in technology.

2. Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The policy for Blackwater School makes explicit to all users (staff and children) what is safe and acceptable and what is not.

The scope of the policy covers fixed and mobile internet and all devices capable of accessing these services which may be used in school or in relation to school work. It should also be noted that the use of devices owned personally by staff and children but brought onto school premises (such as mobile phones, tablets) are subject to the same requirements as technology provided by the school.

3. Expectations of children using the internet

Children's access to the internet is through a filtered service (SENSO), which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

In addition, the following key measures have been adopted by Blackwater School to ensure our children do not access any inappropriate material:

- The school's rules for staying safe online are taken from childnet.com. They are promoted during internet safety sessions and are on display in the classrooms and on every computer trolley in the school.Appendix 2 - Computing rules for Children*
- Children's attention will be brought to the rules annually as well as throughout the year.
- Children using the internet will normally be working in highly-visible areas of the school.
- All online activity is for appropriate educational purposes and is supervised, where possible.
- Children in EYFS and Key Stage 1 will, where possible, use sites pre-selected by the teacher and appropriate to their age group.
- Children in Key Stage 1 and 2 are educated in the safe and effective use of the internet.
- Children in Key stage 2 will be taught how to search and evaluate websites.
- All children are taught how to keep safe, how to collaborate safely, how to evaluate the use of technology for effectiveness, and the basics of copyright (see our Computing Curriculum on our website).

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor TPAT can accept liability under such circumstances.

4. Expectations of staff using the internet

- Children accessing the internet should be supervised by an adult at all times.
- Children are aware of the rules for the safe and effective use of the internet. These are displayed in classrooms and discussed with children regularly.Appendix 2 - Computing rules for Children*
- Recommended websites for each year group can be made available on the school website, in Shared Docs and via email.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school policy should be reported immediately to the Computing Leader or Senior Leadership Team and recorded on CPOMS.
- Passwords should not be shared with anyone, including the network manager. The network manager can override, if necessary, to gain access to someone's folders if deemed appropriate by the headteacher.
- Staff should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of children should, where possible, be taken with a school camera, school phone or iPad and images should be stored on a centralised area on the school network.
- School systems may not be used for unauthorised commercial transactions.
- No program files may be downloaded to the computer from the internet without the Computing Leader's or TPAT's permission.

5. Sanctions of Inappropriate internet use

Incidents of technology misuse which arise will be dealt with in accordance with the school's Relationship (Positive behaviour) policy. Minor incidents will be dealt with by the Computing Leader or Senior Leadership Team and may result in a temporary or permanent ban on Internet use.

Incidents involving safeguarding issues will be dealt with in accordance with school child protection procedures.

All incidents will be logged on CPOMS.

6. Photographs and videos

Parents/carers are asked to fill in a permission form for the school to use their child's photograph on school publicity materials including the school website. See Appendix 1

7. Images taken by parents/carers, legal guardians or family members at a school event

It is made clear at the start of every school event, either verbally and/or written, that the school trusts that if images are taken, then they must be for home use only. It is also requested that if an image of a child is put on social media, then we trust that images of other children must be cropped out. If this is not adhered to, then the school will contact the family and request it be removed.

8. Images taken by staff

Images may be taken by staff using the school's devices. When staff are working with photographic images of children, it is preferable that these are downloaded onto a school computer or encrypted memory stick and not stored on a mobile device such as a camera indefinitely. Where this is not possible, photographs should be deleted at the end of an academic year or when finished with.

9. Images for School Publications

The school will only take and use images that are appropriate and are considered to not be open to misuse. All parents/carers will be asked to complete a form indicating whether they will allow their child's photograph to be used. These will be stored in the office and each class teacher will receive a 'Google Sheet' indicating whether permission has been given or not. If an image of a child is used, the child's full name will not be published, unless permission has been granted. If a name is published, no image will be used without specific consent. Children and parents/carers should be encouraged to recognise the value of group photographs or recordings of school events. The school recognises that images must not be used to cause distress, upset or embarrassment. The school will use photographs that represent the diversity of the children participating. Images of children from the school will not be used to illustrate controversial subjects.

10. Images for the School Website

The school will use the website to celebrate learning, successes and special events that take place in the school. When using images for this purpose the school will ensure that only appropriate images are used and that all relevant permissions are checked. Images can always be removed after the child has left the school at parental request.

11. CCTV

The school uses CCTV in some areas of school property as a security measure. Cameras will only be used in appropriate areas.

12. Children photographing one another

The school owns sets of cameras, iPads and school phones, both still imaging and video imaging as well as devices capable of capturing still and moving images. Staff will supervise and maintain control over any photographing children do during on-school or off-site activities using school devices. As part of online safety, children are explicitly taught about keeping themselves and each other safe.

If children bring phones or smartwatches into school, they must immediately hand them to the office. Children are prohibited from bringing phonesor smartwatches on any visit off site, or residential experiences, but are able to take cameras. Staff are made aware of who has cameras and will monitor their use. If it is found that cameras have been misused, the school will follow the disciplinary procedures. In some cases, it may be necessary for Threemilestone School to contact Children's Social Care and/or the Police.

13. Class, Group and Whole School Photograph

Class and group photographs are taken annually. For clarification purposes, only children whose parents/carers have consented to photographs will be allowed to have class and group photographs. Annual individual professional photographs will be taken for all children unless the school is notified in writing to the contrary.

14. Use of images as part of the EYFS learning journal (Tapestry)

The school uses an online learning journal to trace the assessment of children in the EYFS. Annotated photographs are stored online using a service called 'Tapestry' which is made available to parents/carers. The school has taken the following precautions to ensure the safety of the images and information regarding the children in EYFS:

- All data is stored on secure servers based in the UK and the data uploaded remains the property of the school.
- All devices used for the recording and editing of such images are passcode protected and are able to be remotely wiped in the event of theft.
- Parents/carers have access to their child's learning through an App or via the Tapestry website. This requires registering an email with the school and this is password protected.
- In instances of group learning, photos of children will not be shared with parents/carers unless the parents/carers of all children in the photograph have 'opted in'.
- Parents/carers who opt to receive photos of their children via the App are required to sign to say that they will:
    - Not publish any observations or photographs of their own or other children on any social media site (including Facebook, Instagram and Twitter).
    - Keep their login details within trusted family members.
    - Accept that their child's photograph may appear on their classmate's learning journal account and they may see pictures of other class members on my child's personal account.
- Parents/carers who do not agree to the terms will not be sent images of their child, nor will their child's images be sent to other parents/carers as part of a record of group learning.
- Parents/carers will have the opportunity to discuss these arrangements at the EYFS welcome meeting and by appointment with the EYFS class teachers.
- The EYFS team will have responsibility for uploading the pictures to the online journals and it is the responsibility of the class teachers to ensure that all posts are appropriate for use.

15. Acceptable use of staff mobile phone

Staff mobile phones and/ or smartwatches should be switched off and kept out of sight during classroom lessons and while in the school building or in the grounds, when in the presence of children. Staff may use their phones in the staff room where no children are allowed and during breaks when there are no children in the room. Exceptions may be permitted only in exceptional circumstances, if the adult, specifically requests its use from the Headteacher, or it is needed for work that is being carried out e.g. Mitie caretaker, ICT technician, or other tradesmen. Permission must be sought from the Headteacher prior to the phone being kept on in school and phones should not be taken onto the playground at any times.

Mobile phones or smartwatches should not be used in any manner or place that is disruptive to the normal routine of the school.

16. Unacceptable use of staff mobile phone

Unless express permission is granted, mobile phones or smartwatches should not be used to make calls, send text or media messages, use the internet, take photos or use any other application during school lessons and other educational activities, such as assemblies.

Mobile phones or smart watches must not disrupt classroom lessons with notifications.
Using mobile phones to bully and threaten other staff members is unacceptable and will not be tolerated. In some cases, it can constitute criminal behaviour.

17. Theft or damage of mobile phones or smartwatches

Mobile phones or smartwatches that are found in the school and whose owner cannot be located should be handed to front office reception. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones/ smartwatches..

18. Children's use of mobile phones or smartwatches

The use of mobile phones/smartwatches by children is not permitted on the school premises during school hours. Children may only bring devices to school in exceptional circumstances. All devices are to be handed into the front office and collected as the child leaves the school.

The school accepts no responsibility for children who lose or have their mobile phones/ smartwatches stolen while travelling to and from school. Children's mobile phones/smartwatches are not permitted on school trips.

19. Inappropriate conduct of mobile phone or smartwatch

Any adult/child caught using a mobile phone or smartwatch in an inappropriate manner will face disciplinary action as sanctioned by the Headteacher and/or the governing body.
Mobile phones should not be used to take photographs of the children unless there are exceptional circumstances and then only with the express permission of the Headteacher or a member of the Senior Leadership Team.

School Social Media - please note that this should be read in conjunction with the TPAT Social Media Policy

20. Posts and Comments on the TMS Facebook Page

The Headteacher will decide on and authorise administrators that will be responsible for updating the page on a regular basis, signposting news and information to the Blackwater website.

If followers have any specific concerns, particularly related to their own or other child/children, we ask that they do not post these on the page timeline and encourage them to speak directly to the Headteacher/Class teacher.

While the school does not forbid staff from commenting on the school's posts using their personal accounts, staff are reminded that doing so could compromise the security of their personal details by making them available to all members of the Facebook group.

The page will be moderated daily by administrators that are authorised by the Headteacher.

21. Misuse of posts on the Blackwater Facebook page

In the event that an inappropriate or offensive comment is made it will be recorded by an administrator (screen shot) and brought to the urgent attention of the Headteacher. The school reserves the right to remove any comment or post deemed to be offensive. The Headteacher will speak to the individual(s) involved and explain the purpose and ethos of the page, and why their comment / behaviour is inappropriate or offensive.

In the event that a child is described or named (whether in the main post or within comments), it will be recorded by an administrator (screen shot), immediately deleted and brought to the urgent attention of the Head Teacher. This will be dealt with in a manner appropriate to the Headteacher. Police or Social Care may become involved if appropriate. It may be decided that the person is blocked from the site.

In the event that an inappropriate or offensive comment is made by someone who is unconnected to the school, the Headteacher will respond accordingly. The response will depend on the content of the post but may include contacting the user via private message, deleting the comment and banning the user, or reporting the post to relevant external bodies.

22. Restrictions on the Blackwater Facebook page

The page is designed as a communication tool to engage with parents/carers. It is therefore restricted to people over 18 years of age. Where a parent is under 18 years old, permission will be granted at the discretion of the Headteacher.

23. The use of social networking sites by pupils within school

The school's policy outlines the rules for using technology in school and these rules therefore apply to use of social networking sites. Such sites should not be used/accessed by children in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experiences. If social media sites are used, then staff should carry out risk assessments to determine which tools are appropriate.

Private use of social networking sites by a child is prohibited and it is generally understood that children under the age of 13 are not permitted to be registered on most of the popular social media services.

24. Use of social networking by staff in a personal capacity (to read in conjunction with TPAT’s social media policy)

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must **never** add pupils as ‘friends’ into their personal accounts (including past pupils under the age of 18), unless they are family members..
- Staff are strongly advised not to add parents/carers as ‘friends’ into their personal accounts.
- Staff must not post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teachers’ Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.
- Staff must not message parents/carers privately using a social media site about school business, and if contacted by a parent/carer, must not respond and report it to the Headteacher immediately.
- If staff see on a social media site something which raises safeguarding concerns about a child in the school, then it must be reported to the Headteacher/Designated Safeguarding lead immediately.

25. Internet Safety Awareness

In Blackwater School we believe that, alongside having a written safety policy and code of practice it is essential to educate all users in the safe and effective use of the internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents/carers as it is for children.

26. Internet Safety Awareness for children

Rules for the Acceptable use of the internet are discussed with all children and are prominently displayed in classrooms. In addition, EYFS and Key Stage 1 & 2 children follow a programme of Internet Safety Awareness using a range of resources.

27. Internet Safety Awareness for staff

The Computing Leader keeps informed and updated on issues relating to Internet Safety and attends courses where available. This training is then disseminated to all teaching staff, support staff on a regular basis. The leader also makes regular use of the 'thinkuknow' website which provides training materials.

28. Internet Safety Awareness for parents/carers

Internet safety information for parents/carers is available via the school website. The site hosts a page from parentinfo.org which contains up to date information about safety issues. In addition to this, parents/carers are offered internet safety sessions which they can attend after school or during the day.

29. Use of school computing resources by other agencies

Visiting users may be given access to the school's guest network which has access to the internet. This is password protected. Other agencies using computers on the school premises must agree to this policy.

30. Website Guidelines

The school website is to celebrate exciting learning, promote the school, publish resources, have links to other excellent sites and for home learning.

Rules for responsible use of the school website

- Names of children will never be placed on our website with a photograph that identifies the children.
- No home information (including email addresses) of staff or children is to be published on the website. Any point of contact will be the secretary and Headteacher email addresses or school phone numbers.
- Learning to be displayed will be of a high quality to reflect the status of the school.
- The website will be managed by the administrator and will be kept up to date.

31. Social Software

Chatrooms, blogs and other social networking sites are blocked by the ICT4 filters, so children do not have access to them in the school environment; however, we regard the education of children on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for children.

Instances of cyber bullying of children or staff will be regarded as very serious offences and dealt with according to the school's Relationship (Positive Behaviour) Policy, Antibullying Policy and Safeguarding Procedures as well as being recorded on CPOMS.

Children are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Appendix 1

Dear Parent/Carer,

At Blackwater School we sometimes take photographs of children. We use these photos on the school's website, on display boards around school, in newsletters, on school social media accounts and for the press.

As a TPAT School, Truro and Penwith Academy Trust may also like to use these photos, (which are already on the school website) on the Trust's website, in newsletters, marketing materials, for the press and social media accounts.

We would like your consent to take photos of your child and use them in the ways described above. If you're not happy for us to do this, we will accommodate your preferences.

I am happy for the school to take photographs of my child for use internally within school (school displays & child learning books)	Yes	No
I am happy for photos of my child to be used on the school website. Our TPAT trust may also link to the school website.	Yes	No

If you change your mind at any time, you can let us know by emailing blackwater@tpacademytrust.org , calling the school on 01872 560570, or just popping into the school office. If you have any other questions, please get in touch.

A copy of both the TPAT Social Media Policy and Blackwater Technology Policy is available on the school website.

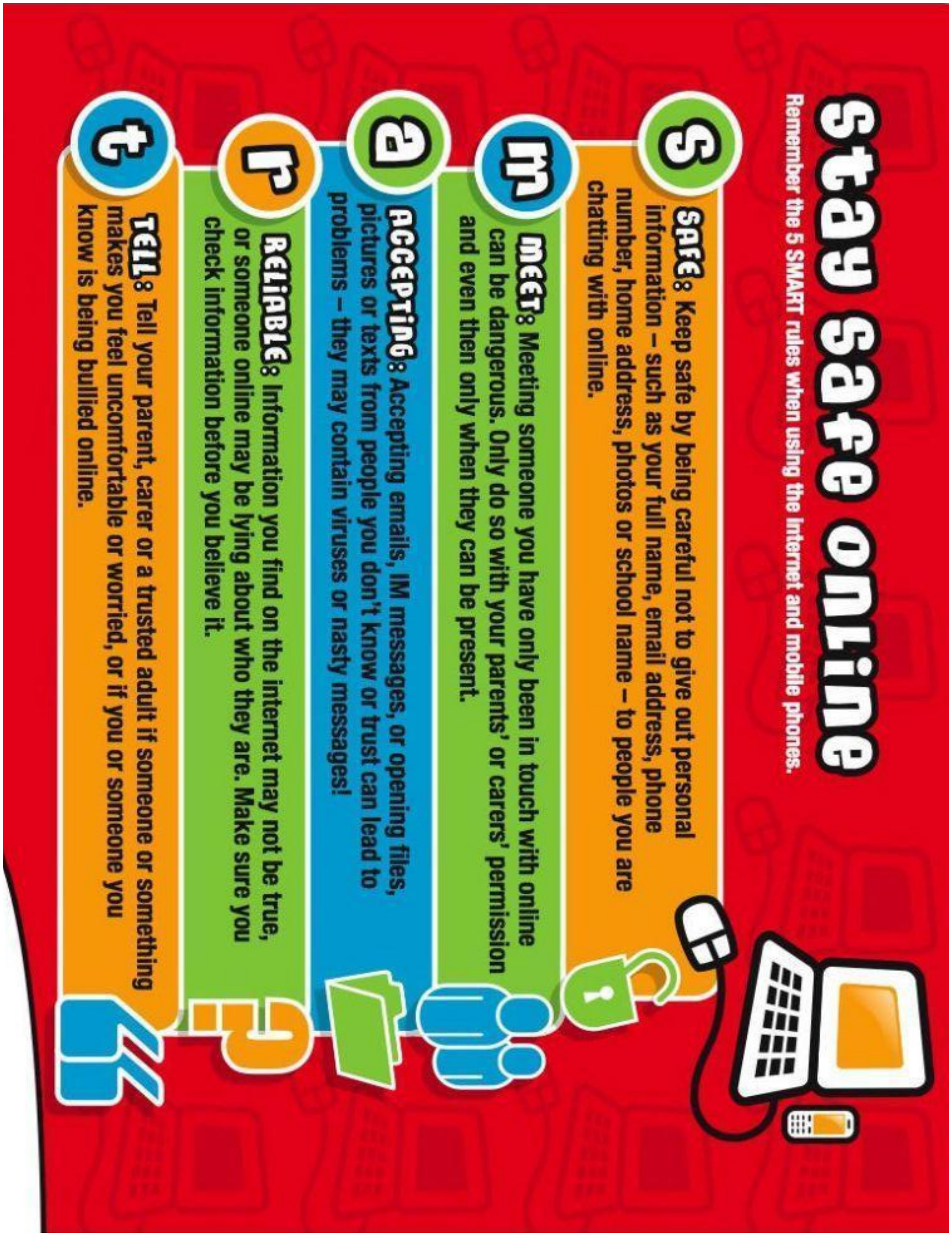
Why are we asking for your consent?

To ensure we are meeting the requirements of general data protection regulation, we need to seek your consent to take and use photos of your child. We and the trust really value using photos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again. For more information on GDPR please follow this link: http://www.tpacademytrust.org/wp-content/uploads/2018/05/GDPR-General-Policy-FINAL.pdf

Child name: ____ Class: ____

Parent or Carer's signature: ____Date: _______________________

Appendix 2 - Computing rules for Children (childnet.com)



stay safe online

Remember the 5 SMART rules when using the internet and mobile phones.

s **SAFE:** Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

m **MEET:** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

a **ACCEPTING:** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

r **RELIABLE:** Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

t **TELL:** Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Appendix 4 TPAT Social Media Policy

1 INTRODUCTION

As a Truro and Penwith Academy Trust school, we ask that all TPAT schools and employees read through and follow this Social Media Policy. Employees of all TPAT schools may be able to access social media services and social networking websites at work, either through company IT systems or via their own equipment.

This social media policy describes the rules of social media use at any TPAT school. It sets out how employees must behave when using the school's social media accounts.

Why This Policy Exists

Social media can bring significant benefits to schools, particularly for building relationships with current and prospective staff, parents and students.

School social media policies have a number of purposes, but their overriding function is to protect staff, students and parents from the many issues that can arise as a result of posting on social networking sites.

Staff may be vulnerable to malicious and defamatory comments (and potentially even threats and abuse) from parents or pupils, and to allegations of grooming and other forms of online abuse. Twenty-one per cent of teachers say they've had derogatory remarks made about them online.

Parents may become involved in online disputes with other parents through social media. They may also potentially put their child and others within the school at risk by sharing photos, videos or other information that could make the children identifiable to others.

Pupils are at risk of cyber bullying and may also become involved in cyberbullying themselves. They are also vulnerable to other serious crimes such as grooming and abduction if they share too much personal information on social media.

Policy Scope

This policy is to be considered in conjunction with schools' own Acceptable Use of ICT policies and TPAT's Staff Code of Conduct.

This policy applies to all employees, contractors and volunteers at any TPAT school who use social media whilst at work – whether for business or personal reasons.

It applies no matter whether that social media activity takes place on school premises, while travelling for business or while working at home.

2 RESPONSIBILITIES

Everyone who operates a school social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

The Headteacher is ultimately responsible for ensuring that the school uses social media safely, appropriately and in-line with the school and Trust's objectives.

However, these people have key responsibilities:

- Marc Hurrell – Assistant Headteacher

3 SOCIAL MEDIA CONTENT

Content to be shared on social media must be related to your school and/or TPAT:

- Events and announcements
- Celebrations and successes
- Articles
- Press releases
- Photographs and videos
- Vacancies

The tone in which you deliver the schools' content on social media should be:

- Light-hearted
- Professional
- Dependent on content

4 GENERAL SOCIAL MEDIA GUIDELINES

Regardless of which social networks employees are using, following these simple rules helps to avoid the most common pitfalls:

- **Know the social network** – employees should spend time becoming familiar with the social network before contributing. It is important to understand what is and is not acceptable on a social media channel before posting anything
- **If unsure, don't post it** – staff should err on the side of caution when posting updates to social networks and

if they feel that an update could cause offense or complaints, they should not post it, and should consult the Headteacher.

- **Be careful with images and personal information** – Employees should consult the Headteacher if unsure of the use of certain student images and should not include any personal information when posting on the school website or social media accounts; full names, addresses, email addresses, phone numbers.
- **Keep a positive tone** – many social media users have gotten into trouble by simply failing to observe basic good manners online. Employees should adopt a pleasant tone when communicating online
- **Look out for security threats** – Staff should be on guard for social engineering and phishing attempts. Social networks can also be used for spam distribution and malware
- **Don't make promises without checking** – some social networks are very public so employees should not make any commitments or promises on behalf of the school or the trust without checking that the school can deliver on the promises. Direct any enquiries to the Headteacher
- **Don't escalate things** – it's easy to post a quick response to a contentious status update or query and then regret it. Employees should take the time to think before responding, and hold back if at all in doubt
- **Keep calm in a crisis** – unfortunately there are occasional incidents which require sensitivity (cyber-bullying, negative comments, external incidents) and it is important not to post on social media until you have the express permission of the Headteacher
- **Be careful with regards to students and staff –** do not accept friend requests from current or ex-students. You must notify the parent if a child sends you a friend request
- **Get permission –** written permission from parents or carers must be obtained before photographs of students or their work are published on the school website and social media
- **Appropriate photography –** Care must be taken when taking and using digital/video images. Students must be appropriately dressed and should not be participating in activities that might bring the individuals or the school into disrepute. Photographs published on the website, or elsewhere that include students, will be selected carefully and will comply with good practice guidance on the use of such images
- **Equipment use –** Images may only be taken on school equipment and the personal equipment of staff must not be used for such purposes

5 USE OF COMPANY ACCOUNTS

This part of the policy covers the use of social media accounts owned and run by the school.

Authorised Users

Only people who have been authorised to use the school's social networking accounts may do so. Authorisation is provided by the Headteacher. Allowing only designated people to use the accounts ensures the school's social media presence is consistent and in-line with guidelines.

Creating Social Media Accounts

New social media accounts in the school’s name must not be created unless approved by the Headteacher. If there is a case to be made for opening a new account, employees should raise this with the Headteacher.

Inappropriate Content and Use

School social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the school or TPAT into disrepute.

6 RESPONSIBLE USE OF SOCIAL MEDIA

Users must **NOT**:

- Create and distribute material that might be defamatory or incur liability for the school and/or TPAT
- Post message, status updates or links to material or content that is inappropriate
- Use social media for any illegal or criminal activities
- Broadcast their own views on social, political, religious or other non-school related matters
- Send offensive or harassing messages to others via social media
- Send or post messages that could damage the reputation or image of the school and/or TPAT
- Discuss colleagues, competitors, students or parents without their approval
- Accept friend requests from current or ex pupils
- Use the full names of students on the school or Trust website, social media or blog, particularly in association with photographs
- Publish photographs of students or their work without the permission of their parents or carers
- Take photographs on a mobile phone or any other personal item
- Use personal social networking sites or blogs when at work

Security and Data Protection

Users should maintain confidentiality and must **NOT**:

- Share or link to any content or information owned by the trust that could be considered confidential or commercially sensitive
- Share or link to any content or information owned by another school or person that could be considered confidential or commercially sensitive
- Share or link to data in any way that could breach the school’s data protection policy

Protect Social Accounts

School social media accounts should be protected by strong passwords that are changed regularly, stored in a spreadsheet known to all involved parties, and shared only with authorised users

Staff must not use a new piece of software, app or service with any of the school’s social media accounts without receiving approval from the Headteacher

7 POLICY ENFORCEMENT

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action. Employees, contractors and other users of the school’s social media may also be held personally liable for violating this policy.