THE ALTERNATIVE SCHOOL GROUP LTD

E-Safety Policy

Author:	**HB**
Date:	**4th September 2024**
To be reviewed:	**Sept 25**
Reviewed:	**Nov ‘16, Dec ‘17, May ’18, Oct ’19, Nov ’19, Feb 20, May 21, Sept 21, May 22, Sept 22; Sept 24**
Version:	**11**

Introduction

Technologies are constantly changing and therefore any policy needs to be as dynamic as possible and in constant review. The school needs to be sufficiently flexible to manage new and emerging technologies, as they may have important educational and social benefits. The policy aims to balance the use of existing and emerging technologies with the necessity of providing safeguards for pupils and staff against risks and unacceptable material and activities. The Alternative School provides internet access for pupils and staff to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Although children may be trusted by their parents and other trusted adults in their home lives with regard to private internet use, schools have a duty to safeguard them and to educate them to use online material safely and responsibly.

The use of technology has, however, become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation - technology often provides the platform that facilitates harm. TAS has therefore developed an effective approach to online safety which empowers each school setting to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate. TAS has a commitment to adapt to emerging technologies while maintaining a focus on safety and educational benefits.

Keeping Children Safe in Education 2024 (Annex C) covers online safety in schools and the guidance states that "the use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; technology often provides the platform that facilities harm. An effective approach to online safety or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."

See also:
The use of social media for on-line radicalisation

• The UK Safer Internet Centre (https://www.saferinternet.org.uk/about)

• CEOP's Thinkuknow website (www.thinkuknow.co.uk)

The main areas of risk for pupils and staff at TAS can be summarised as follows:

Content

- Exposure to inappropriate content.
- Lifestyle websites promoting harmful behaviours.
- Hate content.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms.
- Social or commercial identity theft, including passwords.

Conduct

- Aggressive behaviours (cyberbullying).
- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online, gambling, body image).

- Sexting.
- Copyright (to include plagiarism and illegal downloads).

The school recognises policies and procedures are in place to maintain online safety for both young people and adults. These policies and practices are part of the school's wider safeguarding strategy.

All pupils are required to sign and observe the following Acceptable Use Policies:

- Pupil Acceptable Use Agreement for use of TAS laptops, iPads and tablets (signed when pupils join TAS by pupils and updated by pupils as appropriate)
- Social Media for Staff

All members of teaching staff, support staff and volunteers who have access to the Network at School are required to sign and/or observe the following Acceptable Use Policies:

- Staff/Volunteer ICT Acceptable Use Policy for the use of TAS laptops, iPads and tablets (signed when all members of staff are given access to the Network and updated as appropriate);
- E safety Policy
- Anti-Bullying Policy
- Positive Behaviour Policy
- TAS and social media
- Staff Presence on Social Media Policy
- Cyberbullying Policy
- Data Protection Act (inc GDPR UK) Policy

In addition, members of staff are required to observe the Staff Code of Conduct Policy which includes information about appropriate on-line behaviour as well as the use of photographic, video and audio digital or analogue technology. Staff are made aware that a breach of this or other policies may result in disciplinary action.

This policy provides an overview of the measures TAS has in place to ensure an e-safety environment and sets out its expectations of behaviour in relation to internet use.

<u>Safeguarding and Remote Education during Coronavirus (COVID-19)</u>

With the Covid pandemic starting in early 2020 and the subsequent closure of schools, TAS made the decision to offer a combination of remote learning options that supported all the needs of our pupils, including those who made not have access to unlimited internet access. Staff were given clear guidance with regards to making learning videos or doing live streams to pupils as part of our remote learning offer.

When filming/making videos/live streaming: -

- ? Wear your TAS ID badge, and make sure it is visible.
- ? Be aware of your environment, ensure that there are no family photos etc., in the background. Film against a neutral background where possible.
- ? Do not film family members or friends within your teaching video.
- ? Adopt a smart, casual dress code or wear your TAS school uniform.
- ? During a live stream, pupils and anyone in their household should be appropriately dressed - i.e., not in pyjamas.

- Notify parents/carers when a live stream session is due to take place, in advance of the session.
- Only TAS accounts should be used - e.g., TAS Facebook, or via the TAS website.
- Pupils can also be contacted by using their TAS school e-mail address.
- Staff should only use their work mobiles and/or work e-mail addresses when contacting pupils or parents/carers.

Zoom security update

Zoom implemented two-factor authentication to make video conference safer than ever. Enabling this feature also helps to prevent 'zoom bombing'. Staff were advised to enable the multi-factor authentication and use the security features such as waiting rooms and passwords to increase security.

The school will

• Provide appropriate training in e-Safety for staff and support any staff and pupils having online safety issues

• Provide educational material and support for parents

• Provide policies for e-safety and acceptable use that are clear and easily understood

• Make clear to pupils and staff how they can seek help if they have any concerns

• Make clear what the risks are of using the internet irresponsibly

• Encourage pupils and staff to be discerning regarding material found on the internet

• Make pupils and staff aware of the Acceptable Use Policies and the sanctions in place to enforce them.

Network procedures and practices

The school provides pupils access to the internet via the school iPads. The wifi password must not be given out to pupils. Staff can access the school's wifi.

The school's internet access is provided by GPS.

The iPads are managed through the iPad management system JAMFSchool, provided through JTRS, who are the school's educational technology provider.

Web content filtering is done through OpenDNS to ensure access to inappropriate content is prevented.

In circumstances where the school believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the school reserves the right to inform appropriate authorities and provide documentary evidence.

Pupils should be aware that their files, e-mails and other forms of electronic information storage and communication (including any external storage media which pupils bring into the school) may be scrutinised for the purposes of safeguarding or promoting a child's welfare. This would normally be authorised by the head teacher or assistant head as these are the school DSLs.

Although all staff and pupils are expected to use ICT responsibly and receive specific education to define and encourage responsible use, the school recognises that it has a responsibility to counter any attempts at irresponsible behaviour which may still arise. The School's ICT system is monitored and managed in a number of ways designed to inhibit abuses, specifically:

Web Filtering – the school subscribes to reputable services (Open DNS, JAMFschool) that maintain an online database that categorises websites. Some categories are banned permanently, some are restricted to adults only. The databases of the filtering devices are updated continuously.

Mail Filtering – We use Microsoft Office 365 for email, providing an encrypted connection between the device and Microsoft's servers. Incoming and outgoing Junk and 'spam' emails, and also any containing malware are filtered. It is possible for appropriate staff to send sensitive data (eg safeguarding / medical) by secure email via Egress.

Social Networking sites – access to these is blocked for pupils.

Devices are returned to the office at the end of the working day.

Staff are provided with an iPad by school which can be taken home. These iPads are also managed in the JAMF school management system. An acceptable usage agreement must be signed before a staff member is issued with one.

There is a separate Acceptable Use Policy for pupils having an iPad.

Only staff devices and TAS issued pupil iPads can be connected to the school Wifi system, any changes to this require a password.

Staff need to be observant when pupil devices are being used.

E-Safety is not regarded as the responsibility of the ICT staff alone; Class Teachers are encouraged to discuss issues with their classes as part of the PSHCE programme and subject teachers to remind classes of best practice whenever online resources are being used. This includes staying safe online and the dangers of cyber-bullying and sexting – even if pupils in a particular faith community are not meant to use mobile phones or have limited access to the internet.

<u>Prevent Strategy</u>

We are very much aware of our responsibilities under the prevent strategy. Any staff with concerns about a child should pass these on without delay to the safeguarding DSL or deputy DSL. If neither of these are available, then the member of staff should contact Kirsty Swierkowski.

Staff having concerns regarding sites which the children access must report these to Mark Walton or Kirsty Swierkowski.

<u>Expectations of pupils and parents beyond the school</u>

When a pupil is at home, families bear responsibility for the guidance of their children. The school expects the use of ICT by its pupils, even when at home, to comply with the school's stated ethos. Material downloaded in the home, posted on an internet site from a home computer, or transmitted to/from a mobile phone when a pupil is at home, can impact significantly upon the life of pupils at school. We ask all parents/guardians to co-operate with the school in the education of their children in the use of ICT.

<u>ICT and E-Safety External Adviser:</u>

As part of our commitment to maintaining a safe and secure online environment, The Alternative School has appointed an ICT and E-Safety External Adviser. This expert plays a pivotal role in advising our school community on matters related to information and communication technology, as well as e-safety. The adviser collaborates closely with our staff, ensuring that our internet safety measures remain current and effective. They provide guidance on best practices, emerging threats, and strategies for promoting responsible online behaviour among both students and staff. The ICT and E-Safety External Adviser also assists in the regular review and enhancement of our internet safety policy, ensuring that it aligns with UK regulations and best practices. Their expertise contributes significantly to our ongoing efforts to safeguard the well-being of our school community in the digital age.

E safety focus group (KS, MW, ST)

• Assume overall responsibility for e-safety.

• Ensure that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.

• Are aware of procedures to be followed in the event of a serious e-safety incident.

• Takes day to day responsibility for e-safety issues and has a co-ordinator / leading role in establishing and reviewing the school e-safety policy.

• Promotes an awareness and commitment to e-safeguarding throughout the school community.

• Ensures that e-safety education is embedded across the curriculum.

• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

• To ensure that users may only access the school's networks using the relevant username and password, and to encourage the use of strong passwords which are regularly changed.

• To ensure that provision exists for misuse detection and malicious attack (e.g., keeping virus protection up to date).

• To ensure the security of the school ICT system.

• To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.

• To ensure that web filtering devices are maintained and updated on a regular basis.

• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

All Staff

• To embed e-safety issues in all aspects of the curriculum and other school activities.

• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

• To read, understand and help promote the school's e-safety policies and guidance.

• To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.

• To report any suspected misuse or problem to the DSL.

• To maintain an awareness of current e-safety issues and guidance e.g., through CPD.

• To set a safe, responsible and professional example in their own use of technology.

• To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones etc.

Parents

• To support the school in promoting e-safety.

• To read, understand and promote the school Pupil Acceptable Use Agreement with their children. This is sent out to all parents in the first half of the term.

• To consult with the school if they have any concerns about their children's use of technology.

• To read and understand the Acceptable Use Policy for pupils.

• To understand the importance of reporting abuse, misuse or access to inappropriate materials.

• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

• To know and understand school policy on the taking / use of images and on cyber-bullying.

• To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

For Pupils

The school provides a variety of devices with internet access to help you with your learning. There is also 'Office 365', which gives you email which you can use to contact your friends and family -and also cloud storage where you can store documents which you can work on at school or at home. All pupils are given email addresses at the start of the year.

So that everyone at TAS uses the computers safely and with due consideration for others, we need to have some rules which you must follow.

We have tried to keep these rules as simple as possible so that everyone can understand them.

Using the Computers

• If I am worried about anything I find on the computers I will tell a member of staff.

• I will only access the computer system using the username and password I have been given.

• I will not give my username and password to anyone else.

• I will use the computers sensibly and not interfere with any of the wiring or the settings of

the computers. When I have finished I will leave the computer tidy for the next person.

• I will not attempt to access others' files or emails.

• I will not bring in CDs, DVDs or USB drives from outside school and try to use them on the school computers without permission.

• I understand that the computers are provided primarily for work.

Using the Internet

• If I see anything or receive any messages that concern me, I will tell a member of staff immediately because this will help protect other pupils and me.

• I will not deliberately search for inappropriate material on the internet.

• I understand that all my use of the computers is recorded, and that the ICT staff may check my computer files and the sites that I visit.

• I will not give away any personal information to any sites on the internet. If I am not sure about this, I will ask a member of staff.

• I will not download any files or applications without permission.

• I will not attempt to use any chat rooms or social networking sites.

• I will not copy or download work from the internet and claim it as my own.

Using e-mail and Office 365

• I will only use the school Office 365 e-mail system. Messages I send will be polite and reasonable.

• If I receive an email that I am worried about or that I find unpleasant, I will not delete the email but will tell a member of staff as soon as possible.

• I will only e-mail people I know. For my own safety I will not give any personal details such as my email address, home address or phone number to people or organisations that I do not know.

• I will not use the email system to send games or inappropriate material to other people.

• I will only use the Cloud Storage (OneDrive) for storing work-related material.

• I understand that use of my school email / Office 365 account from home or elsewhere is still subject to the terms of this Policy.

Remote Learning using MS Teams and other software provided by TAS.

• I understand that video meetings using Zoom may be recorded and stored securely.

• I understand that whilst engaging in remote learning, the Acceptable Use Policy still applies. I will use the system responsibly with due consideration for others.

Personal Devices

• If permitted to use a device at school, I understand that this is only to assist in my classroom learning. It is not to be used for playing games. Emails must be sent via my school address and should only be work-related.

• Use of my personal device at school is still subject to the Acceptable Use Policy.

• I will not let anyone else use my device. I will ask a teacher if I need help using it in the classroom.

Deliberate Misuse

• I understand that deliberate misuse of any ICT device may result in action being taken.

Remember that these rules are for your own safety. If you are concerned about anything, tell a teacher.

Roles and Responsibilities for Online Safety

The E-Safety focus group, Kirsty Swierkowski, Mark Walton, Stewart Townsend have the responsibility of ensuring that the technical provision and ICT infrastructure across the school have appropriate safeguards in place to filter and monitor appropriate content and to alert the school to any potential safeguarding issues.

The school have now commissioned an ICT & E-safety adviser - Stewart Townsend.

In each campus, the Headteacher has responsibility for:

- ensuring that all teaching and relevant support staff sign and uphold the relevant Acceptable Use Policies.
- ensuring that all pupils and parents sign and uphold the relevant Acceptable Use Policies.

If pupils/children discover unsuitable sites, they are instructed to alert a member of the staff. Staff are then instructed to alert their DSL and Kirsty Swierkowski. The URL (address) and content are reported to the Internet Service Provider via Kirsty Swierkowski.

Education of the Pupils/Parents/Staff About E-Safety

Pupils are taught in E-Safety sessions what internet use is acceptable and what is not as appropriate to their age and setting. In particular, they are informed that they must not reveal personal details (including their address or telephone number) or others' details in e-mail communication or via a personal web space; neither must they arrange to meet anyone. Pupils are encouraged to report all issues and concerns to a member of the teaching team, who will escalate the matter to a member of the Management Team and who, in turn, will pass the matter on to Kirsty Swierkowski.

Issues around cyberbullying are discussed in PSHCE/Collective Reflective lessons. Any form of bullying or harassment is strictly forbidden, and sanctions are used as appropriate for those who engage in cyber/text bullying. When publishing material to websites and elsewhere, pupils are taught to consider the thoughts and feelings of those who might view the material. Action is also taken against any person who brings the school into disrepute through publication of inappropriate electronic materials/communications.

Pupils are taught that they may only use approved e-mail accounts on the school system and may only communicate to staff via school accounts. Pupils are required to inform a teacher if they receive an offensive e-mail. The teacher will then escalate the matter to their DSL or to Kirsty Swierkowski.

Staff safeguarding training includes information about online safety. Parents are given information about online safety at the Parent/Carer Days, school newsletters and other school letters/publications.

Key advice to protect staff:

All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times.

- Ensure you understand the school's policies on the use of social media. Child-net's "For You as a Professional" has more information on what to be aware of (www.childnet.com/teachers-and-professionals/for-you-as-a-professional)
- Do not leave a computer or any other device logged in when you are away from your desk.
- Enabling a PIN or passcode is an important step to protect you from losing personal data. and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by pupils.
- Keep all passwords and login details secret and ensure you lock your computer or office if away from your desk.
- Make sure you understand how to secure any websites or social networking services you use.
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the 'Safer internet advice and resources for parents and carers'.
- Keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online, it is much easier to deal with this as soon as it appears. 'The UK Safer Internet Centres Reputation' mini site has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Always think carefully before you post and don't post any information (photos, videos, comments) publicly online that you wouldn't want employers, colleagues, pupils or parents/carers to see. Just because a profile might be set to 'private' it doesn't mean that someone else can't copy or share it without your knowledge.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Also consider if it could bring you, the school's or someone else's reputation into disrepute: posting something inappropriate, obscene or threatening online could lead to criminal, civil and/or disciplinary action.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not add or accept friend requests from pupils (past or present) or their parents/carers on any personal social networking accounts. Discuss any issues with this (for example any pre-existing relationships) with the school.
- Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not use your own personal devices or personal social networking profiles to contact pupils or parents/carers.
- Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school contact details.
- On school trips, staff should use a school mobile phone and never their own.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites, for example, Dropbox and YouTube.
- Ensure that the school's rules and policies regarding the use of technologies by pupils and staff are enforced. Make sure you read and understand the school's Cyberbullying, ICT Acceptable Use, TAS and social media and Staff Presence on Social Media Policies.
- Follow the remote learning policy in regard to remote teaching over the internet.

The School's Technical Provision & Infrastructure

All laptops and iPads that are used by pupils must have Open DNS installed on them. Mark Walton will support Kirsty Swierkowski with installing this onto devices.

iPads must be set up with the following restrictions.

- Pupils are allowed the Passcode only to access the iPads.
- Only Kirsty Swierkowski and Mark Walton will be allowed to install apps.
- iPads and iPencils must be signed out of the office and returned at the end of the day – the teacher who signed out the iPad and iPencil are responsible for them. Remember that iPads are high value items.
- They can only be charged in the office.
- At the end of the day, they will be locked away in a filing cabinet in the office.
- If a pupil is doing anything inappropriate on the iPad, it must be reported to Kirsty Swierkowski or Mark Walton as changes to the settings may be needed.
- The iPads must be used for educational purposes only.
- Pupils are not allowed to use social media apps on them.
- Pupils will be charged for any damage caused to the iPads and iPencils as per the ICT Acceptable Use policy they must sign before they use the TAS iPads.

When setting up the iPads, the following restrictions must be set

- Go to >settings >general >screen time >use screen time passcode and set passcode as 9725
- Choose >always allowed and remove the following apps from this screen
    - Messages
    - Facetime
    - Contacts
    - Find friends
    - iTunes store
    - Mail
    - Music
    - Stocks
    - Apple TV
- Choose >content and privacy restrictions and switch this option on
    - >iTunes and App Store Purchases and Don't Allow >installing apps, >deleting apps and in app purchases.
    - Switch on the option for require password to >always require.

- Choose >allowed apps and switch off the following apps
    - Mail
    - Facetime
    - iTunes Store
- Choose >content restrict and change the settings to these
    - >Ratings for – United Kingdom
    - >Music, podcasts and news – clean
    - >Music profiles and posts – off
    - >Films – 12
    - >TV programmes – caution
    - >Books – clean
    - >Apps – 12+
    - >Web content – Limit adult websites and select >Never allow websites and add: Facebook, Snapchat, Instagram, Twitter, You Tube, Reddit, Tumblr, Buzz Feed, Cool Maths Games, Friv, Pac Man.
    - >Content restrictions >explicit language – Don't allow.
    - >Game centre >multiplayer games – Don't allow.
    - >Game centre >adding friends – Don't allow.
    - >Game centre > screen recording – Don't allow.
- >Advertising – Don't allow.
- >Media and Apple music – Don't allow.
- >Passcode changes – Don't allow.
- >Account changes – Don't allow.

- A maximum of 1 fixed computer per classroom.
- To be sited in full view of teacher at all times.
- 30 min time slot per pupil allowed.
- A log kept of all pupils accessing the internet.
- Wi-Fi password MUST not be passed to pupils.
- Pupils must not access teacher laptops or any other device within school.
- Teacher laptops must be password protected and locked down automatically every minute not used, or alternatively used only in the office.
- Exam laptop to contain exam data only and must be password protected, plus supervised at all times through the exam. Storage in a secure place.
- D of E laptop to be password protected and supervised at all times.
- All staff to be vigilant around pupils who are using their own data to access the internet and a log kept and reported up of anything suspicious or of allowing other pupils to use this data.

School website

- The Proprietor, supported by the heads, takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained.
- The school web site complies with statutory DfE requirements.
- Most material is the school's own work; where other's work is published, or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Responding to incidents of misuse at TAS:

- The school will take all reasonable precautions to ensure online safety
- A flow chart will be displayed in school to advise on how to deal with any incidents of misuse (see Appendix 1: Responding to incidents of misuse flow chart).
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes by following the Responding to Incidents of Misuse flowchart (Appendix 1).
- Any suspected online risk or infringement should be reported to the Headteacher.
- A record must be made following any incidents of misuse so that the issue/incident can be reviewed by SLT during their meeting unless the incident puts a pupil or member of staff at immediate risk in which case the DSL must be immediately informed.
- Support is actively sought from other agencies as needed (i.e., the local authority, London Grid for Learning (LGfL), UK Safer Internet Centre helpline, Child Online Exploitation Protection (CEOP), Prevent Officer, police, Internet Watch Foundation (IWF) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- The police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Review and Monitoring

- The E-Safety policy will be reviewed annually or sooner when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy, and it has been agreed by the management team. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Further references

- ➢ E-safety within the School Inspection Framework, Ofsted, September 2014
- ➢ Childnet, http:/www.childnet.com/
- ➢ E-safety Support, https://www.e-safetysupport.com/
- ➢ UK Safer Internet Centre, http://www.saferinternet.org.uk/
- ➢ Child Exploitation and Online Protection Centre, https://www.ceop.police.uk/
- ➢ Prevent, http://www.preventforschools.org/

- ➢ 360⁰ Safe, https://www.360safe.org.uk/
- ➢ Internet Watch Foundation, https://www.iwf.org.uk/

The Management of Personal Data

The school abides by the 2018 General Data Protection Act when processing personal data and technical and organisational measures are in place to safeguard personal data from destruction, loss, unauthorised access or disclosure. There is a separate Data Protection Policy, produced by the Safer Recruitment and Data Protection Officer, Heather Blake.

Appendices

Appendix 1 - Responding to incidents of misuse – flow chart

Appendix 2 - Record of reviewing devices/internet sites (responding to incidents of misuse)

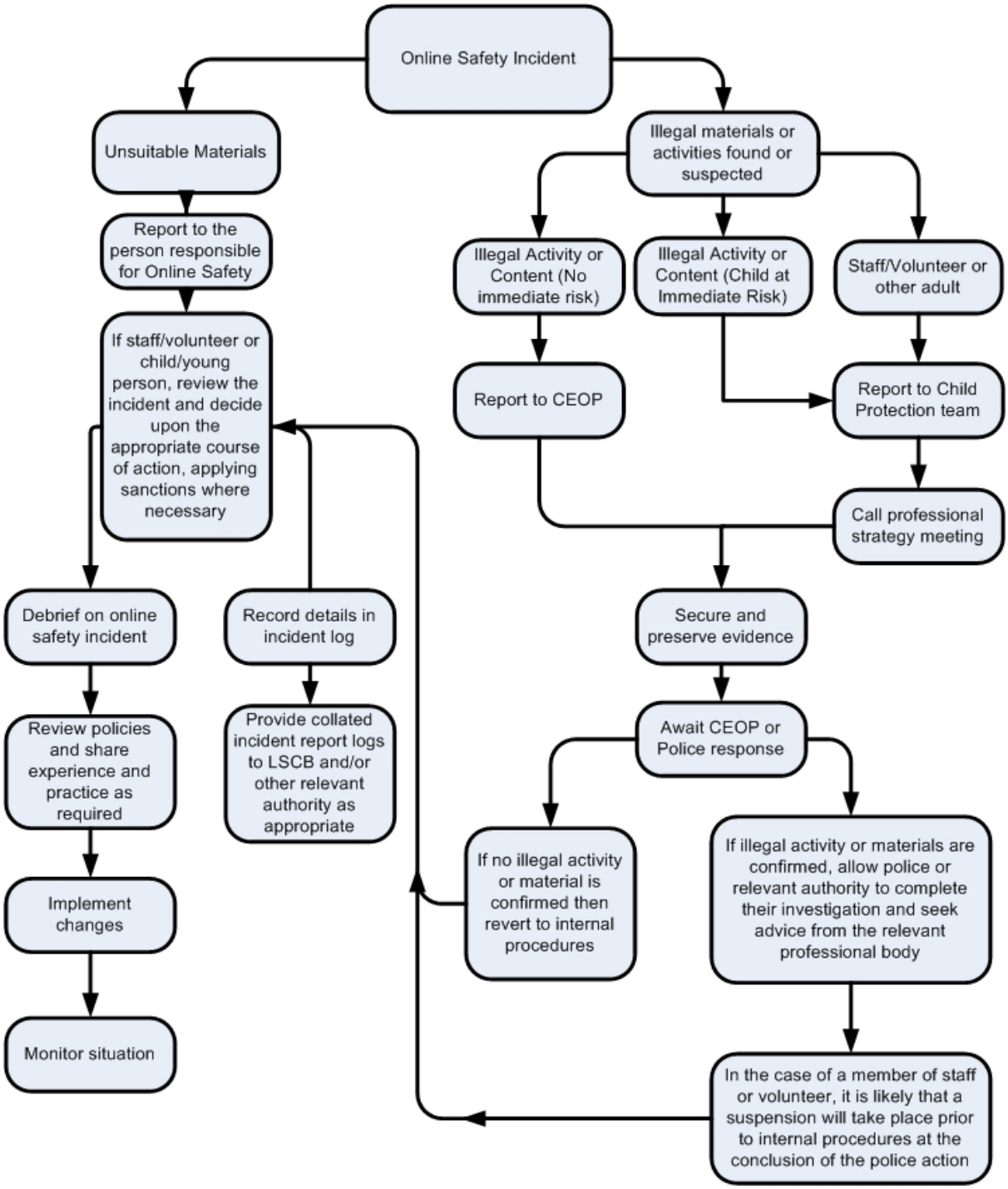
Appendix 3 - Pupil Acceptable Use Agreement for the use of TAS laptops, iPads and tablets

Appendix 4 - Staff/Volunteer ICT Acceptable Use Agreement for the use of TAS laptops, iPads and tablets

Appendix 5 – Barnoldswick iPads

Appendix 1:

Responding to incidents of misuse – flow chart



Source: South West Grid for Learning, 360° Safe

Appendix 2:

Record of reviewing devices/internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address/device and reason for concern

Conclusion and Action proposed or taken

Source: South West Grid for Learning, 360⁰ Safe

Pupil Acceptable Use Agreement for use of TAS laptops, iPads and tablets

TAS accepts that internet use is an important part of a young person's life but has a duty to teach our pupils how to be safe and responsible whilst using the internet and other digital technology both in school and at home.

TAS will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

For my own personal safety:

- I understand that TAS will monitor my use of the internet in school.
- I will keep my username and password safe and secure.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not share personal information about myself or others when on-line.
- I will tell a member of staff if I see something online or get sent a message that makes me feel uncomfortable.
- I will not use the *school computers for social media,* on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g., YouTube), unless I have permission of a member of staff to do so.
- I will respect other’s work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email (due to the risk of the attachment containing viruses).
- I will not install programmes on school computers, nor will I try to alter computer settings.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will reference my sources when using the internet for any BTEC or other work as required by the exam board.
- I will treat all equipment with respect.
- I will pay for any damage caused to any TAS equipment.
- I will log out of any equipment before sharing it with others.
- I will hand in all equipment at the end of the session.

Name of Pupil: .....

Signed: .....

Date: .....

Appendix 4

Staff/Volunteer ICT Acceptable Use Agreement for the use of TAS laptops, iPads and tablets.

TAS accepts that internet use is an important part of everyday life as a member of staff/volunteer at TAS we have a duty to be safe and responsible whilst using the internet and other digital technology both in school and at home.

For my professional and personal safety:

- I understand that TAS will monitor my use of the internet in school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g., on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's Social Media policy.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops/mobile phones/tablets) in school, I will follow the rules set out in this agreement, in the same way as if I was using school devices. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses in relation to TAS communication.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or that may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read the staff acceptable use policies on the use of the internet, social media and mobile devices and have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name of Staff/ Volunteer: .....……..

Signed: .....……
……

Date: ……..

Appendix 5

Barnoldswick iPads

iPad 1 (Light blue case)

Passcode	scoutandboo1
Case colour	Light blue
Model	MR7J2B/A
Serial number	F9FYP4VXJF8M
Storage	128gb
Date of birth	16 May 1980
iPad name	TAS Pendle 1
Email	TASPendle1@icloud.com
Password	Umpalumpa123@!
PIN	9725

iPad 2 (Dark blue case)

Passcode	scoutandboo2
Case colour	Dark blue
Model	MR7J2B/A 6th Gen
Serial number	F9FXCH7YJF8M
Storage	128gb
Date of birth	16 May 1980
iPad name	TAS Pendle 2
Email	TASPendle2@icloud.com
Password	Umpalumpa123@!
PIN	9725

iPad 3 (Green case)

Passcode	scoutandboo3
Case colour	Green
Model	MR7J2B/A 6th Gen
Serial number	F9FWND59JF8M
Storage	128gb
Date of birth	16 May 1980
iPad name	TAS Pendle 3
Email	TASPendle3@icloud.com
Password	Umpalumpa123@!
PIN	9725

iPad 4 (Purple case)

Passcode	scoutandboo4
Case colour	Purple
Model	MR7J2B/A 6th Gen
Serial number	
Storage	128gb
Date of birth	16 May 1980
iPad name	TAS Pendle 4
Email	TASPendle4@icloud.com
Password	Umpalumpa123@!
PIN	9725

- Pupils are allowed the Passcode only to access the iPads.
- Only Kirsty Swierkowski and Mark Walton will be allowed to install apps.
- iPads and iPencils must be signed out of the office and returned at the end of the day – the teacher who signed out the iPad and iPencil are responsible for them. Remember that iPads are high value items.
- Pupils cannot sign out iPads.

- They can only be charged in the office.
- At the end of the day, they will be locked away in a filing cabinet in the office.
- If a pupil is doing anything inappropriate on the iPad, it must be reported to Kirsty Swierkowski or Mark Walton as changes to the settings may be needed.
- The iPads must be used for educational purposes.
- Pupils are not allowed to use social media apps on them.
- Pupils will be charged for any damage caused to the iPads and iPencils as per the ICT Acceptable Use policy they must sign before they use the TAS iPads.

When setting up the iPads, the following restrictions must be set.

- Go to >settings >general >screen time >use screen time passcode and set passcode as 9725
- Choose >always allowed and remove the following apps from this screen
    - Messages
    - Facetime
    - Contacts
    - Find friends
    - iTunes store
    - Mail
    - Music
    - Stocks
    - Apple TV
- Choose >content and privacy restrictions and switch this option on
    - >iTunes and App Store Purchases and Don't Allow >installing apps, >deleting apps and in app purchases.
    - Switch on the option for require password to >always require
- Choose >allowed apps and switch off the following apps.
    - Mail
    - Facetime
    - iTunes Store
- Choose >content restrict and change the settings to these
    - >Ratings for – United Kingdom
    - >Music, podcasts and news – clean
    - >Music profiles and posts – off

    - >Films – 12
    - >TV programmes – caution
    - >Books – clean
    - >Apps – 12+
    - >Web content – Limit adult websites and select >Never allow websites and add: Facebook, Snapchat, Instagram, Twitter, You Tube, Reddit, Tumblr, Buzz Feed, Cool Maths Games, Friv, Pac Man
    - >Content restrictions >explicit language – Don't allow
    - >Game centre >multiplayer games – Don't allow
    - >Game centre >adding friends – Don't allow
    - >Game centre > screen recording – Don't allow
- >Advertising – Don't allow
- >Media and Apple music – Don't allow
- >Passcode changes – Don't allow
- >Account changes – Don't allow

Date	Name	iPad	Time In	Time Out

Barnoldswick iPad Log

iPad 1 – light blue	iPad 2 – dark blue
iPad 3 – green	iPad 4 - purple

Date	Name	Signed by pupil to say pupil understands	iPad	Pencil	Keyboard	Time In	Time Out	Any damage on return

Classroom iPad log

iPad use in the classroom

I understand that I am allowed to use the TAS iPad in school. I have signed the school ICT agreement and understand that if I lose or damage the iPad, iPencil or keyboard I will have to pay for the equipment. If I use the ICT equipment inappropriately, I will not be allowed to use it.

Name (print)……..

Signed: ……...

Date: ……...