e-Safety Policy

TORQUAY ACADEMY

E Safety Policy

The e-safety Policy is part of the School Development Plan and relates to other policies including those for Computer Security, anti-bullying and for child protection & safeguarding.

The school's e-safety coordinator is Mr Pugh

Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

The e-safety Policy and its implementation will be reviewed annually.

Teaching and Learning

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- For children with social, familial or psychological vulnerabilities, further consideration will be taken to reduce potential harm.

Benefits of the Internet

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Professional development for staff through access to national developments,
- Access to learning wherever and whenever convenient.

Internet to Enhance Learning

Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will Pupils Learn How to Evaluate Internet Content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular, it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems Securely

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

Email

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive emails.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain messages is not permitted.

Website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

- The Principal or nominee will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Students Images and Work

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

Social Networking, Social Media and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms, instant messenger and many others.

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

Electronic Communication with Students

Staff and helpers can also be susceptible to risks from social networking. The following guidelines are designed to protect staff:

1. Staff should not become “friends” with students on Facebook.
2. Facebook community groups used for school purposes should be declared to and authorised by your SLT line manager.
3. Facebook school community groups should not contain personal information relating to staff.
4. Staff should be aware that students and parents may follow them on Twitter. They should take this into account when posting information to the site. Posting information which could embarrass or compromise other members of staff should be avoided.
5. Staff should only use their school email address for communication with students.

Filtering

- The school’s broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Safeguarding officer who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The school’s access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from the network manager.

Managing Filtering

- The school will work in partnership with South West Grid for Learning to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents may be useful to identify patterns and behaviours of the students.

Data Protection

- Personal data will be recorded, processed, transferred and made available according to The General Data Protection Regulation 2016 (‘GDPR’).

Authorising Internet Access

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

- Secondary students will apply for Internet access individually by agreeing to comply with the School e–Safety Rules or Acceptable Use Policy.

Internet Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor SWGfL can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Incidents of Concern

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

Safety Complaints

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any inappropriate content, comments, images or videos online.

Cyberbullying

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via

mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or
    - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.

Mobile Phones

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA , MP3 Players etc. are considered to be an everyday item in today's society mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

- The use of mobile phones and other personal devices by students and staff in school will be covered in the school Acceptable Use Policy and Behaviour Policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team without* the consent of the pupil or parent/carer.
- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms or toilets.

*

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/279245/searching_screening_confiscation_advice_feb14.pdf

Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children and young people.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

- All users will be informed that network and Internet use will be monitored.
- An e–Safety programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE and ICT programmes covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

How will the Policy be Discussed with Staff

- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will Parents' Support be Enlisted

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and
- suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.