Torre C of E Academy

E-Safety Policy 2021

Writing, Monitoring and Reviewing:

This e-safety policy was developed by a working group made up of:

- Headteacher - Mrs Sue Julyan
- Former Computing co-ordinator – Miss Michelle Lewis
- Current Computing coordinator - Mr. Ben Cowling
- Other staff - Mrs Laura Kendell – Deputy Head, Mrs Vicki Thomas – Child Protection Officer.
- Governors

Since then, the policy has been adjusted by current computing co-ordinator - Mr. Ben Cowling

This e-safety policy was approved by the *Governing Body on:*	20th June 2019
History: E-safety and acceptable use policy last written in:	2007 (updated in 2012 by Computing coordinator) Review and updated by ML May 2019 Review and updated by BC, June 2021.
The implementation of this e-safety policy will be monitored by:	BC, SJ and Governors
Monitoring will take place at regular intervals:	Annually
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Summer Term 2022

The school will monitor the impact of the policy using:

- Logs of reported incidents are logged on Behaviour Watch and monitored by BC.
- Regular surveys/questionnaires completed by children, staff and parents.

Scope of the Policy:

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents /carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

Torre Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of Governors will include:

- Meetings with the E-Safety Coordinator
- Monitoring of e-safety incident logs which have been made on Behaviour Watch.
- Reporting to relevant governors/board/committee/meeting

Headteacher and SLT:

- The headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The headteacher and computing coordinator are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The headteacher and senior leaders are responsible for ensuring that the e-safety coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

E-Safety Coordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Receives reports of e-safety incidents via Behaviour Watch and monitors the log of incidents to inform future e-safety developments.
- Meets with the e-safety governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends a relevant meeting/committee of Governors.
- Reports regularly to the Senior Leadership Team.
- Provides resources and training for all members of staff to ensure their e-safety training and knowledge if up to date.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school/ academy e-safety policy and practices.
- This will be done by completing yearly the NOS online training for e-safety.
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)

- They report any suspected misuse or problem on Behaviour Watch and therefore, to the Headteacher or computing coordinator for investigation/action/sanction.
- All digital communications with children/parents/carers should be on a professional level and only carried out using official school systems and also complies with GDPR regulations.
- E-safety issues are embedded in all aspects of the curriculum and other activities. E-safety resources (particularly those provided by computing coordinator through The National Online Safety Award) are delivered termly to each class.
- Children understand and follow the e-safety and acceptable use policies.
- Children, represented by the School Council, have an input in the writing of the Children Friendly E-Safety Policy.
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- The security of personal devices whilst on the school premises is in-line with this policy by ensuring that personal devices are not accessible to children and kept in a locked secure place.

Child Protection / Safeguarding Designated Person:

Should be trained in e-safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

This training is provided by the NOS (National Online Safety Award) and the DSL will complete training specific to their role.

Children:

- Are responsible for using the school digital technology systems in accordance with E-safety rules at Torre. Please see
  Torre C of E Academy Chromebook Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Children are responsible for any personal device that, on direction of their class teacher, is brought into school to support learning in the classroom. These devices will be kept on their desk or in a charging cabinet, where they are accessible when necessary and when supervised.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying. They will also understand that smart watches are not appropriate to wear during the school day.
- Should 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.

Parents and Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, parent/carer forums, letters, websites and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Their children's personal devices which are used in the classroom to support learning.

Parents will also be offered online training through the NOS.

The Computing Curriculum at Torre C of E Academy:

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of the computing curriculum at Torre and the children revisit e-safety every half term. E-safety is the first topic covered each year in every year group.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Children should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- It is ensured that children are safe from terrorist and extremist material when accessing the internet in school. Suitable filtering is in place.
- The use of devices with 3G / 4G will be carefully monitored and only used when necessary and pre-planned with potential risks considered.
- As you can see from the wide range of opportunities whereby electronic devices can be used in the daily running of our school and the delivery of the computing curriculum, communications technologies are rapidly developing and have the potential to enhance learning in many ways. The following table shows how our school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff and other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought into school	✔				✔ *			
Use of mobile phones in lessons		✔ *						✔
Use of mobile phones in social times	✔							✔
Photos to be taken on personal devices of other children				✔				✔
Use of instant messaging		✔						✔
Use of social networking sites		✔						✔
Use of blogs	✔				✔			

Please note - Where mobile phones are referenced it is used to include other devices such as iPads/tablets or wearable technology such as smart watches. The use of smart watches is not appropriate in school due to risks of loss and damage and of misuse in the same way as mobile phones or tablets.

* Some staff use their phones as a method of communicating in Team Teach emergencies; the risks have been managed by SLT and this has been approved.

** Phones are not permitted in KS1 or in the lower parts of KS2. Year 5 and 6 are permitted to bring their phones into school and these are kept in a secure locked draw/cupboard until the end of the day.

Education for our families:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- E-safety parent drop in sessions
- Training through the NOS website
- Letters, newsletters, website,
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications

Education and The Wider Community:

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety.
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide e-safety information for the wider community
  Supporting community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their e-safety provision.

Education and Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events or online training (e.g. from LA/other relevant. organisations) and by reviewing guidance documents released by relevant organisations. The E-Safety coordinator will also keep up to date training through the NOS website and ensure that all staff are aware of new training to complete. Staff will then be expected to complete the NOS training.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/ team meetings/INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice/ guidance/training to individuals as required.
- The E- Safety Coordinator / Officer will monitor who has received training.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff. They will be offered the NOS online e-safety training.

Technical – infrastructure/equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented with the help and support of ITEC. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices.
- The headteacher / LA officer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. The email system of Egress will be used to email these documents. Internal emails can be used to share appropriate information about children and teacher professional judgement can be used here.

Use of digital and video images:

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images **of their**

own children at school events for their own personal use (as such use is not covered by GDPR) To respect everyone's privacy and in some cases protection, these images should not be published and made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students/pupils in the digital / video images. These images are not to include photos of other children.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies and parental consent, concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents can declare on the data consent form (in writing) if they do not want their child to be photographed.
  - Staff should not use their own personal devices to take photos of children. School devices should be used and photos to be deleted afterwards.
  - All of the above to be regularly communicated to parents (via an Online Safety briefing for parents to attend and by ensuring that this information is available on our website and during other appropriate times – such as performances / class assemblies etc).
  - Parents are all asked to complete the data consent form to ensure we have an up to date representation of their wishes regarding the processing of pupils personal data (including images and videos).

Social Media - Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held

responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment.

School staff should ensure that:

- No reference should be made in social media to children/parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.