Creating Tomorrow Trust

E-Safety Policy 2026 -2028

Purpose

This policy is written to ensure all Staff, Parents, Governors and Trustees and Students are fully aware of the purpose and nature of the E-Safety Policy.

New technologies inspire children to be creative, communicate and learn.

However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter.
Creating Tomorrow Trust will endeavour to highlight benefits and risks of using technology and provides safeguarding and education for users to enable them to control their online experience.

Complied by: ITBP	**Date:** Mar 26
Committee: Trust Board	**Date agreed by:** Jun 26
Review Cycle: Every 2 Years	**Review Date:** Mar 28

Creating Tomorrow Trust

E-Safety Policy 2026 -2028

Role	Purpose
Trustees and Governors	To provide strategic oversight and assurance that e-safety across the Trust is lawful, proportionate and aligned with safeguarding duties, ensuring systems, policies and practice protect students, staff and the organisation; ensuring effective governance, policy impact (including wellbeing), and confirmation that technology, filtering, reporting and incident-management processes are robust and consistently applied across all schools and the college.
Leaders	To ensure e-safety is embedded in all aspects of school and college operation by implementing safe, lawful, proportionate and trauma-informed practice when managing online behaviours, incidents and digital systems. Ensuring that leaders oversee staff training, filtering, monitoring, reporting and curriculum practice, to meet statutory guidance, and promote a culture of wellbeing, safeguarding, digital responsibility and consistent incident management.
Staff	Clarifying the important role that staff play in educating students, promoting safe online practices, and responding promptly and accurately to any online safety concern, ensuring student wellbeing and safeguarding remain central. To ensure staff are aware of their duty to safeguard students and use technology safely and professionally by modelling responsible online behaviour and following all e-safety expectations when they access digital tools. Ensuring that staff are aware that they must follow Trust procedures for acceptable use, filtering, email, mobile devices, recording incidents, and protecting personal data.

Wellbeing at Creating Tomorrow Trust

At Creating Tomorrow Trust, we believe that when our people thrive, our learners and communities thrive too.

Physical, emotional and mental wellbeing are essential to a thriving, collaborative and values-driven organisation, and we are committed to creating an environment where every colleague feels supported, respected and able to flourish.

We recognise that wellbeing needs can change over time, and anyone may experience challenges. We work together with openness, compassion and trust, ensuring that help is accessible when it is needed.

Health and wellbeing are everyone's responsibility, and we encourage a positive culture where concerns can be raised without judgement. The Trustees take their duty of care seriously and are committed to ensuring that support for all employees is available through:

- Effective and supportive line management
- A fair and manageable workload
- A professional, safe and inclusive working environment
- Access to wellbeing and employee support services through our Employee Assistance Programme:
  - *08000 856 148*
  - *educationsupport.org.uk*

We are committed to continuous improvement. **All Trust policies are reviewed for their impact on staff wellbeing**, ensuring our values are reflected not only in what we say, but in what we do. Together, we create tomorrow by caring for one another today.

Creating Tomorrow Trust

E-Safety Policy 2026 -2028

1. Links to other policies and national guidance

1.1 The following policies and procedures should also be referred to

- Safeguarding Policy
- Whistleblowing Policy
- Relationship (behaviour) Policy
- Mobile Devices Policy
- Acceptable Use of ICT Policy
- Staff Code of Conduct
- Remote Working Policy
- Data Protection Policy
- Social Media Policy

1.2 The following local/national guidance should also be read in conjunction with this policy:

- PREVENT Strategy HM Government
- Keeping Children Safe in Education
- Teaching Online Safety in Schools DfE
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

2. Learning and Teaching

2.1. We believe that the key to developing safe and responsible behaviours online, not only for pupils / students / learners (from this point forward will use the term student) but everyone within our communities, lies in effective education.

2.2 We know that the internet and other technologies are embedded in our students' lives, not just in our schools and college but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the internet brings.

2.3 How we help prepare our students:

- We will provide a curriculum and lessons which has e-Safety embedded throughout.
- We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities.
- We will discuss, remind or raise relevant e-Safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Our schools / college will model safe and responsible behaviour in their own use of technology during lessons.

- We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, students will be guided to use age appropriate search engines. All use will be monitored and students will be reminded of what to do if they come across unsuitable content.
- Students will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying guidance.
- Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as NSPCC.

3. Remote/Home Learning

3.1. We will endeavour to ensure that students continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and learning portal

3.2. If our schools / college are forced to move to remote learning then any communication via Zoom, Teams, WhatsApp will only be carried out with the approval of a member of the senior leadership team.

3.3. Students must uphold the same level of behavioural expectations, as they would in the classroom setting, following the school / college Relationship Policy

3.4. Any significant behavioural issues occurring on any virtual platform must be recorded, reported and managed as per the school / college procedures, which may include temporarily suspending access to group online learning. For all minor incidents, these should be addressed using the usual restorative approaches.

3.5. Staff should be mindful that when dealing with any incidents online, opportunities to discuss and repair will not be the same as if the student was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure their child is emotionally well supported.

3.6. For further information please refer to the Remote Working Policy.

4. General Note for incident at school / college or online

4.1. At every stage the student should be involved in, or informed of, the action taken

4.2. Urgent or serious incidents should be referred straight to the headteacher/Principal, or a member of SLT

4.3. If necessary, refer to the other related internal policies and procedures e.g. Child Protection & Safeguarding, Anti-Bullying

4.4. Staff should follow the usual process for recording concerns (Safeguarding - My Concern, Behaviour - Arbor). Entries should be factual and action/follow up also recorded.

5. Staff Training

5.1. Staff will receive regular information and training on e-Safety issues, as well as updates as and when new issues arise.

5.2. As part of the induction process all staff will receive information and guidance on the E Safety Policy, e-security and reporting procedures.

5.3. All staff will be made aware of individual responsibilities relating to the safeguarding of learners within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

5.4. All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

6. Managing ICT Systems and Access

6.1. The school / college will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive.

6.2. All users will be made aware that they must take responsibility for their use and conduct while using the school ICT system and that such activity will be monitored and checked.

6.3. At Key Stage 1, pupils will access the network using an individual username and a class password which the teacher supervises.

6.4. At Key Stage 2 and above, pupils will have an individual user account with an appropriate password which will be kept secure. They will ensure that they log out after each session.

6.5. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.

6.6. Members of staff will access the internet using an individual ID and password, which they will keep secure (staff are not to share passwords with other staff or students). They will ensure that they log out after each session and not allow students to access the internet through their ID or password.

7. Managing Filtering

7.1. The school / college has an internet filtering system in place which is managed by the Trust IT Team. Banned phrases and websites are identified.

7.2. The school / college have a clearly defined procedure for reporting breaches of filtering.

If staff or students discover an unsuitable site, or a website with potentially illegal content, it must be reported immediately to a member of the SLT who will inform the IT team.

7.3. The incident must also be recorded via My Concern as a safeguarding concern and a DSL will support any student effected.

- The Trust will report such incidents to appropriate agencies including; Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).
- Any amendments to the filtering, or block and allow lists, will be checked and assessed by the Headteacher/Principal prior to being released or blocked.
- The evaluation of online content materials is a part of learning and teaching in every subject and will be viewed as a whole-school requirement across the curriculum.

8. E-Mail

8.1. Staff and students should only use approved email accounts allocated to them by the school / college and should be aware that any use of the Trust email system will be monitored and checked.

8.2. Staff should not use personal email accounts for professional/work related purposes, especially to exchange any school / college related information or documents or to email parents/carers.

8.3. Staff should not send personal emails to students, but may be required to send work related emails such as Teams invites, school work etc. These must be within work hours using the Trust email system.

8.4. Students are encouraged to immediately tell a member of staff, or trusted adult, if they receive any inappropriate or offensive emails.
8.5. Irrespectively of how students or staff access their school / college email (from home or within the organisation), our Trust policy still applies.

8.6. Chain messages or advertising are not permitted and must not be forwarded on to other Trust owned email addresses.

9. Social Networking – (Please see social media policy)

9.1. Staff will not post content or participate in any conversations which will be detrimental to the image of the schools / college or Creating Tomorrow Trust.

9.2. Staff who hold an account should not have parents or students as their 'friends'. Doing so may result in disciplinary action as is a breach of the staff code of conduct and safeguarding procedures.

- We understand that staff may have contacts who are family members with students in the school, or pre-date employment; this must be disclosed to the Headteacher/Principal

9.3. Blogs or social media sites should be password protected and run from the school / college website with approval from the Senior Leadership Team.

10. Publishing Content Online - (Please see social media policy)

10.1. Students will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.

10.2. Students' full names will not be used anywhere on the website, particularly in association with photographs and video.

10.3. Written permission is obtained from the parents/carers before photographs and videos are published.

10.4. Any images, videos or sound clips of students must be stored on the school / trust network and never transferred to personally-owned equipment.

10.5. Students and staff are only permitted to use Trust owned portable devices to store images/video/sound clips of students. Storing on these devices are temporary whilst data is transferred to the Trust network and then must be deleted from those devices.

11. Mobile Phones and Devices (please see Mobile Devices Policy)

11.1. General use of personal devices

11.1.1. Generally, mobile phones and personally-owned devices will not be used during lessons or school time. They should be switched off or silent at all times.
11.1.2. When there is agreed use of personal devices (to play music to aid concentration, or for planned activities) they will be used as per agreed protocols (no access to internet etc)
11.1.3. No images or videos will be taken on personally owned mobile phones or devices.
11.1.4. In the case of school / college productions, Parents/carers are permitted to take pictures of their child only in accordance with agreed protocols. Schools are responsible for making this clear at the beginning of an event.
11.1.5. The sending of abusive or inappropriate text, picture or video message is forbidden. Please refer to the Mobile Devices Policy for further information.

11.2. Students use of personal devices

11.2.1. Students will be expected to keep their mobile device switched off and kept in their bags, or hand them to a member of staff for collection at the end of the day.
11.2.2. The device will be kept securely in a locked cupboard or drawer during the school day.
11.2.3. Please see the Mobile Devices Policy in regards to supporting students who do not follow the policy

11.3. Screening, Searching and Confiscation (please see the Trust Approach to the Use of Reasonable Force and Searching Students)

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the student has a device prohibited by the school / college rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break academy rules,
- commit an offence,
- cause personal injury, or

- damage property

11.4. Staff use of personal devices

11.4.1 Staff are not permitted to use their own mobile phones or devices for contacting students or their families, within or outside of the setting, in a professional capacity.
11.4.2. Staff will not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use school provided equipment for this purpose.
11.4.3. If a member of staff breaches the policy then disciplinary action may be taken.
11.4.4. Mobile phones and personally owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the senior leadership team for emergency circumstances.

12. CCTV

12.1. The school / college may use CCTV in some areas of property as a security/safeguarding measure.

12.2. Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

12.3. Please refer to the CCTV Policy for further information

13. General Data, Data Protection (GDPR) and e-safety - (Please see Data protection policy and privacy polies)

13.1. GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

13.2. Data must always be:

- Processed lawfully, fairly and transparently
- Collected for specific, explicit and legitimate purpose
- Limited to what is necessary for the purposes for which it is processed
- Accurate and kept up to date
- Held securely
- Only retained for as long as is necessary for the reasons it was collected.

13.3. Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school / college population and external stakeholders, particularly, but not exclusively: students, parents, staff and external agencies.

13.3. Personal and sensitive information should only be sent by email when on a secure network, and sent with protection such as encryption or password protected.

13.4. Personal data should only be stored on secure devices. In the event of a data breach, the school / college will notify the Trust's Information Manager (IM) immediately, who may need to inform the Information Commissioner's Office (ICO).

14. Authorising Internet access

14.1. All staff must read this policy before using any of the trust's IT resources.

14.2. All parents will be required to grant permission prior to their child being granted internet access within the school / college.

14.3. The school / college maintains a current record of all staff and students who have been granted access to our internet provision.

15. Support for Parents

15.1. Parents attention will be drawn to the schools'/college's e-Safety policy and safety advice in newsletters, websites and e-Safety information workshops.

15.2. The websites will be used to provide parents with timely and meaningful information about their child's education lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

16. Radicalisation Procedures and Monitoring

16.1. It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach.

16.2. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Designated Safeguarding Lead).

16.3. Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet, and key word reporting is in place to ensure safety for all staff and students.

17. Sexual Harassment

17.1. Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats) is child on child abuse and will not be tolerated across our Trust. Our schools and college follow and adhere to national guidance.

17.2. Sexual harassment is likely to:

- violate a child's dignity
- make them feel intimated, degraded or humiliated and/or
- create a hostile, offensive or sexualised environment.

17.3. Any reports of online sexual harassment will be taken seriously, must be recorded as a safeguarding concern via My Concern and as an incident of child on child bullying via Arbor. The police and Children's Social Services may be notified.

18. Responses to Incident of Concern

18.1. An important element of e-Safety is the ability to identify and deal with incidents of concern, including the confidentiality of information.

18.2. All staff, volunteers and students have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school /college has incident reporting procedures in place and staff are expected to record:

- Safeguarding concerns via MyConcern
- Behaviour incidents via Arbor

There may be times when one incident is required to be recorded on both systems, for example in the case of child on child abuse - this is a behaviour incident (perpetrated by a student) and a safeguarding incident (affecting a student)

19. Misuse of the Internet

19.1. Misuse of the internet will be managed as per the Relationship policy and may result in consequences such as withdrawal of access privileges, and in extreme cases an exclusion (internal or external).

19.2.The school / college also reserve the right to report any illegal activities to the appropriate authorities.