****

**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 Academies 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.

Compiled by: Kevin Latham

Agreed by Directors – Jan 2022

SIGNED DATE

Review Date – Jan 2024

**Wellbeing in our Trust**

The responsibility for managing e-Safety can be challenging and so this document aims to set out procedures to be followed to minimize what can be difficult process.

We are all affected by poor physical and mental health at times during our lives and it is important the appropriate support is available in a timely manner.

Health and wellbeing is everyone’s responsibility and we encourage an open and honest culture whereby anyone can discuss any issues they may have.

The Trustees of Creating Tomorrow take the health and wellbeing of all employees seriously and are committed to supporting our staff. The Trustees ensure that support for staff is available through:

* Effective line management
* Commitment to reducing workload
* Supportive and professional working environments
* Employee support programs
  + Health Assured (confidential counselling support available through Perkbox account).
  + The Teacher Support Line telephone number 08000 562561 or website [www.teachersupport.info](http://www.teachersupport.info)

**Links to other policies and national guidance**

The following policies and procedures should also be referred to

* Safeguarding Policy
* Whistleblowing Policy
* Behaviour Policy
* Staff Code of Conduct
* Remote Working Policy
* Data Protection Policy

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

* PREVENT Strategy HM Government
* Keeping Children Safe in Education DfE September 2020
* Teaching Online Safety in Schools DfE June 2019
* Working together to Safeguard Children
* Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of

Violent Extremism.

**Learning and Teaching**

We believe that the key to developing safe and responsible behaviours online, not only for pupils but

everyone within our communities, lies in effective education. We know that the internet and other

technologies are embedded in our pupils’ lives, not just in our academies but outside as well, and we

believe we have a duty to help prepare our pupils to safely benefit from the opportunities the

internet brings.

* We will provide a curriculum and lessons which has e-Safety related lessons 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 pupils 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.

* Pupils well be taught how to use a range of age-appropriate online tools in a safe and

effective way.

* Our academies will model safe and responsible behaviour in their own use of technology

during lessons.

* We will teach pupils 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, pupils will be guided to use age appropriate

search engines. All use will be monitored and pupils will be reminded of what to do if they

come across unsuitable content.

* Pupils 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 Policy.

* Pupils 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.

**Remote/Home Learning**

* We will endeavour to ensure that pupils continue to receive a good level of education

‘beyond the classroom’ by providing a range of resources via our website and learning portal

* If our academies choose to communication with pupils over the coming weeks/months via

Zoom, Teams, Skype etc then it is important that this is only carried out with the approval of

the Heads of School. Pupils must uphold the same level of behavioural expectations, as they

would in a normal classroom setting.

* Any significant behavioural issues occurring on any virtual platform must be recorded,

reported and appropriate sanction imposed, which may include temporarily suspending

access to group online learning. For all minor behavioural incidents, these should be

addressed using the normal restorative approaches.

* Staff should be mindful that when dealing with any behavioural incidents, online,

opportunities to discuss and repair harm will not be the same as if the child or young person

was in school. Therefore, it may be necessary to have a discussion with the parents,

regardless how minor the incident, to ensure the child is emotionally well supported.

* Further information please refer to the Remote Working Policy.

**General Note for incident in school or online** ·

* At every stage the child should be involved in or informed of the action taken
* Urgent or serious incidents should be referred straight to the Head of School, or a member of SLT
* If necessary, refer to the other related internal policies e.g. Anti-Bullying, Child Protection, E

Safety etc ·

* Normal recording systems on MYCONCERN should continue. Entries should be factual and

action/follow up recorded also.

**Staff Training**

Our staff receive regular information and training on e-Safety issues, as well as updates as and

when new issues arise.

* As part of the induction process all staff receive information and guidance on the E Safety

Policy, e-security and reporting procedures.

* All staff will be made aware of individual responsibilities relating to the safeguarding of

children 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.

* All staff will be encouraged to incorporate e-Safety activities and awareness within their

curriculum areas.

**Managing ICT Systems and Access**

* The academies will agree on which users should and should not have internet access and the

appropriate level of access and supervision they should receive.

* All users will be made aware that they must take responsibility for their use and behaviour

whole using the school ICT system and that such activity will be monitored and checked.

* At Key Stage 1, pupils will access the network using an individual username and a class

password which the teacher supervises.

* At Key Stage 2, 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.

* All internet access will be undertaken alongside a member of staff or, if working

independently, a member of staff will supervise at all times.

* Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to

access the internet through their ID or password.

**Managing Filtering**

* The academies have a filtering system in place which is managed by the Trust IT Team. Banned phrases and websites are identified.
* The academies have a clearly defined procedure for reporting breaches of filtering.
* If staff or pupils discover an unsuitable site, it must be reported immediately.
* If users discover a website with potentially illegal content, this should be reported

immediately. The academy 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 prior to being released or blocked.

* The evaluation of online content materials is a part of teaching and learning in every subject

and will be viewed as a whole-school requirement across the curriculum.

**E-Mail**

* Staff and pupils should only use approved email accounts allocated to them by the academies and should be aware that any use of the academy email system will be monitored and checked.
* Staff should not use personal email accounts for professional purposes, especially to

exchange any school related information or documents or to email parents/carers.

* Staff should not send personal emails to pupils, but may required to send work related emails such as teams invites, school work etc. These must be within work hours using the academies email system.
* Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any

inappropriate or offensive emails.

* Irrespectively of how pupils or staff access their academy email (from home or within the

academy), our academies policies still apply.

* Chain messages are not permitted or forwarded on to other academy owned email

addresses.

**Social Networking**

* Staff will not post content or participate in any conversations which will be detrimental to the image of the academies or the Creating Tomorrow Academies Trust. Staff who hold an account should not have parents or pupils as their ‘friends’. Doing so will result in disciplinary action or dismissal.
* Blogs or social media sites should be password protected and run from the academies

website with approval from the Senior Leadership Team.

to multi-academy trust

**Pupils Publishing Content Online**

* Pupils will not be allowed to post or create content on sites unless the site has been

approved by a member of the teaching staff.

* Pupils’ full names will not be used anywhere on the website, particularly in association with

photographs and video.

* Written permission is obtained from the parents/carers before photographs and videos are

published.

* Any images, videos or sound clips of pupils must be stored on the academies network and

never transferred to personally-owned equipment.

* Pupils and staff are not permitted to use portable devices to store images/video/sound clips

of pupils.

**Mobile Phones and Devices**

**General use of personal devices**

* Mobile phones and personally-owned devices will not be used in any way during lessons or

school time. They should be switched off or silent at all times.

* No images or videos will be taken on mobile phones or personally owned devices.
* In the case of academy productions, Parents/carers are permitted to take pictures of their

child in accordance with academies protocols - signing a form that they will not publish of

the photographs or videos on social networking sites.

* The sending of abusive or inappropriate text, picture or video message is forbidden.
* Please refer to the Mobile Devices Policy for further information.

**Pupils’ use of personal devices**

* Pupils’ who need to bring a mobile phone in to the academies can only do on request

received from parents explaining the reason that a mobile phone would be needed.

* The phone will be kept in the academy office during the school day.
* Pupils who do not follow the policy relating to the use of mobile phones will not be permitted to bring their mobile phones in.

**Screening, Searching and Confiscation**

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or

parental permission, if there is a suspicion that the pupil has a device prohibited by the academies’

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

**Staff use of personal devices**

* Staff are not permitted to use their own mobile phones or devices for contacting children or

their families within or outside of the setting in a professional capacity.

* Staff will not use personal devices such as mobile phones or cameras to take photos or

videos of pupils and will only use school provided equipment for this purpose.

* If a member of staff breaches the policy then disciplinary action may be taken.
* 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 granted by a

member of the senior leadership team in emergency circumstances.

**CCTV**

* The academies may use CCTV in some areas of academy property as a security/safeguarding measure.
* Cameras will only be used in appropriate areas and there is clear signage indicating where it

is in operation.

* Please refer to the CCTV Policy for further information

**General Data, Data Protection (GDPR) and e-safety**

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and

legitimate purposes; 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.

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.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding

all of the school population and external stakeholders, particularly, but not exclusively: pupils,

parents, staff and external agencies.

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.

Personal data should only be stored on secure devices. In the event of a data breach, the academy

will notify the Trust’s Information Manager (IM) immediately, who may need to inform the

Information Commissioner’s Office (ICO).

**Authorising Internet access**

* All staff must read this policy before using any of academies IT resources.
* All parents will be required to grant permission prior to their children being granted internet

access within academies.

* The academies maintain a current record of all staff and pupils who have been granted access to our internet provision.

**Support for Parents**

* Parents attention will be drawn to the academies’ e-Safety policy and safety advice in newsletters, the academies’ websites and e-Safety information workshops.
* The websites will be used to provide parents with timely and meaningful information about their children’s school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

**Radicalisation Procedures and Monitoring**

It is important for us to be constantly vigilant and remain fully informed about the issues which

affect the region in which we teach. 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). Regular monitoring and

filtering is in place to ensure that access to appropriate material on the internet and key word

reporting it in place to ensure safety for all staff and pupils.

multi-academy trust

**Sexual Harassment**

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.

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).

Any reports of online sexual harassment will be taken seriously, and the police and Children’s

Services may be notified.

Our academies follow and adhere to the national guidance.

**Responses to Incident of Concern**

An important element of e-Safety is the ability to identify and deal with incidents of concern

including the confidentiality of information. All staff, volunteers and pupils 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 has incident reporting procedures in place and

record incidents of an e-Safety nature on MyConcern.

**Sanctions**

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of

access privileges, and in extreme cases, suspension or expulsion, in accordance with the Behaviour

or Trust Discipline Policy. The academies also reserve the right to report any illegal activities to the

appropriate authorities