Creating Tomorrow Academies Trust

Trust Acceptable Use Policy 2021

Purpose

This policy defines the roles of key people within the Trust and Schools, and the responsibilities for everyone, in ensuring the safe use of Trust technology.

Compiled by: Kevin Latham

Agreed by Directors – June 2021

SIGNED DATE

Review Date – June 2022

Creating Tomorrow Academies Trust

Trust Acceptable Use Policy 2021

Wellbeing in our Trust

The responsibility for managing public finances 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.educationsupport.org.uk

Contents

1. Purpose

The purpose of this policy is to ensure that all staff, students, visitors, families, governors and Trustees are aware of their responsibilities when using information technology within the Trust and when using technology to communicate.

2. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole Trust community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within a Trust or educational setting. The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT.

The purpose of the Acceptable Use Policy is to clearly identify for the whole Trust community:

- The steps taken in the Trust to ensure the-Safety of students when using the internet, e-mail and related technologies
- The Trust's expectations for the behaviour of the whole Trust community whilst using the internet, e-mail and related technologies within and beyond the Trust
- The Trust's expectations for the behaviour of staff when accessing and using data.

3. Scope of policy

The policy applies to all Trust based employees, including individuals working in a voluntary capacity, students, students, governors and trustees. All Trusts are expected to ensure that non-employees on site are made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the Trust/educational settings' disciplinary procedures and code of conduct applicable to employees and students.

Where this policy is applied to the Trust Leadership Team (CEO, CFO or COO of the Trust) or a headteacher, the Chair of Trustees will be responsible for its implementation.

Where the Committees of the Trust wishes to deviate from this proposed policy or adopt any other policy, it is the responsibility of the Committees of the Trust to arrange consultation with appropriate representatives from recognised trade unions and professional associations.

4. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all Trust employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

- The Children Act 2004
- Trust Staffing (England) Regulations 2020
- Working Together to Safeguard Children 2018
- Education Act 2011
- Safeguarding Vulnerable Groups Act 2017
- Keeping children safe in education 2020

All safeguarding responsibilities of Trusts and individuals referred to within this Acceptable Use Policy includes but is not restricted to the legislation listed above.

5. Responsibilities

CEO and Trustees

The CEO and Trustees have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the CEO and Trustees should:

- Ensure there is an e-Safety policy in place that supports the safeguarding of all children.
- Ensure the Headteacher / lead of the educational establishment designates an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately.
- Ensure that e-safety is embedded within all child protection training, guidance and practices.
- The CEO will be the e-safety contact for staff not based in education establishments.

Headteacher and Local Governing Body (LGB)

Responsibility for the implementation of safeguarding policy and procedures is at the local establishment level and therefore to meet these responsibilities the Headteacher and LGB should:

- Designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within each establishment.
- Provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.

- Promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the Trust development plan.
- Share any e-safety progress and curriculum updates at meetings of the LGB and ensure that all present understand the link to child protection.
- Report issues of concern and update the LGB and CEO on a regular basis.
- Ensure that e-safety is embedded within all child protection training, guidance and practices.
- Elect an e-Safety Governor to challenge the establishment about e-Safety issues.
- make employees aware of the LSCBN Inter-agency Child Protection Procedures at www.lscbnorthamptonshire.org.uk

E-Safety Lead

The nominated e-Safety lead should:

- Recognise the importance of e-Safety and understand the establishments and Trust's duty of care for the-Safety of their students and employees.
- Establish and maintain a safe ICT learning environment within the establishment.
- Ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- With the support of the Network Manager or IT Subject Leader, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing Trust equipment.
- Report issues of concern and update the headteacher on a regular basis.
- Liaise with the Anti-Bullying, Child Protection and ICT leads so that procedures are updated and communicated and take into account any emerging e-safety issues and technological changes.
- Co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.
- Maintain an e-Safety Incident Log to be shared at agreed intervals with Headteacher and LGB at Trust meetings.
- With the support of the Network Manager or ICT Lead, implement a system of monitoring employee and student use of Trust issued technologies and the internet where appropriate (establishment must decide how they wish to do this-i.e. monitor upon concern raised, random monitoring through collection of devices, or purchase of specialist monitoring software e.g. Impero)

Individual Responsibilities

All Trust based employees, including volunteers under the age of 18, must:

- Take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- Ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.
- Report any e-Safety incident, concern or misuse of technology to the e-Safety lead or head of the establishment, including the unacceptable behaviour of other members of the Trust community.
- Use Trust ICT systems and resources for all Trust related business and communications, particularly those involving sensitive student data or images of students. Trust issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the headteacher, for example, due to equipment shortages.
- Ensure that all electronic communication with students, parents, carers, employees and others is compatible with their professional role and in line with Trust protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with students and their families.
- Not post online any text, image, sound or video which could upset or offend any member of the whole Trust community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- Protect their passwords/personal logins and log-off the network wherever possible when leaving workstations unattended.
- Understand that network activity and online communications on Trust equipment (both within and outside of the Trust environment) may be monitored, including any personal use of the Trust network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out, should be detailed in the establishment's local IT Policy.
- Understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.
- Protecting students against all messages of violent extremism using any means or medium to express views that:
    a. encourage, justify or glorify political, religious, sexist or racist violence
    b. subscribe to rigid and narrow ideologies that are intolerant of diversity, leaving those who hold them vulnerable to future radicalization
    c. foster hatred which might lead to inter-community violence in the UK
    d. seek to provoke others to terrorist acts
- Respecting copyright and the privacy and ownership of other people's work and Acknowledging the source of information used.

- Questioning the reliability of material published on the Internet.
- Images of students and staff will only be taken, stored and used for Trust purposes in line with Trust policy and not be distributed outside the Trust network without the permission.
- Not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Trust community.
- Not attempting to bypass the internet filtering system.
- Not using proxy sites.
- Not using chatrooms or social network sites while in school / college.
- Understand the protocols when using video conferencing - refer to Trust video conferencing policy.

6. Acceptable use of Trust Equipment

Users are expected to use computers, printers and other technologies within Trust or other settings in an appropriate manner. This includes:

- Only using ICT systems in Trust, including the Internet, Firefly, email, digital video, mobile technologies, etc. for Trust purposes.
- Students and teachers logging on to the Trust network/ VLE (Firefly) using own username and password.
- Not revealing passwords to anyone and changing them every six months.
- Only opening and / or deleting your own personal files.
- Only printing suitable text and images which are required for educational purposes.
- Ensuring memory sticks or other transferable data files have been virus checked to minimise issues of virus transfer.
- Not downloading or installing software onto Trust technologies.

7. Appropriate use of e-mail

The use of e-mail within the Trust is an essential means of communication. The Trust gives all users their own e-mail accounts to use for all Trust business as a work-based tool. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. However Trust e-mail is accessed (whether directly, through webmail when away from the office or on non-Trust hardware) all Trust e-mail policies apply.

Acceptable use of e-mail includes:

- Keeping email passwords secure.
- Ensuring that all ICT communications with students, teachers or others is responsible and sensible.
- Using language which is appropriate.
- Not sending file or image attachments which would cause offence.
- Not sending emails to large groups of students without prior permission.

- Not forwarding chain letters/ emails using Trust email.
- Not revealing any personal details about self or others.
- Immediately reporting the receipt of any offensive e-mail.
- Never opening attachments from an untrusted source.
- Never opening links in emails from an untrusted source
- Ensuring all Data protected information is sent securely e.g. via egress, or password protected.
- Not placing a forwarding rule on Trusts email accounts so that Trust emails are being redirected to personal accounts and vice versa.

8. Acceptable use of Mobile Devices and Other Technologies

When mobile phones are used in unauthorised circumstances they may be removed from the individual and kept securely by a member of the senior leadership team for the rest of the day (please refer to the DfE guidance Searching, screening and confiscation at school).

Please refer to the Trust Mobile Device Policy for details on the charging of mobile devices in Trust.

Acceptable use of:

(i) Personal mobile devices

- Access can be made to Trust email on mobile devices such as PDAs and smartphones, but such devices must be encrypted. Encryption will be enforced via password protection in the first instance. Any device that has access to Trust's email system without a password will be denied, until such time that device meets requirement set out in this policy.
- Users can access the Trust's guest wireless network by entering a temporary login provided by Admin Staff
- Users must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording is not allowed. Personal mobile devices must not have any images, video or sound recordings of students or workforce. Trust Email ONLY.
- The Trust is not responsible for any theft, loss or damage of any personal mobile device. If you are accessing Trust emails on your mobile device and it is lost or stolen, you MUST report this to the Trust as soon as possible so that your email access can be secured.

(ii) Trust issued mobile devices

- Where the Trust has provided a mobile device, such as a laptop, iPad or mobile phone, this equipment should only be used primarily to conduct Trust business both inside and outside the Trust environment.
- Equipment provided by the Trust should not be used to store large quantities of personal files.

- Any personal files stored on mobile devices must comply with the provisions of the Data Protection legislation.
- Mobile devices should only be used to connect to a digital projector or Apple TV under authorised circumstances.
- Professional documents which contain Trust-related sensitive or personal information (such as children's reports and data, including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones) must be protected by encryption. Encryption must be used when transferring any personalised documents onto portable devices. (e.g USB pen drives, external hard drives)

9. Acceptable use of video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in Trust there is access if required for students to use:

- Digital cameras
- Video cameras

In all possible situations Trust issued equipment must be used. If personal equipment is used permission must be granted by the Headteacher or CEO of the Trust.

- Personal images should not be uploaded onto personal space (My Documents) or on to the Trust Cloud based Environments without express permission.
- It is recommended that permission is sought prior to any uploading of images to check for inappropriate content.
- Uploaded images should not have a file name of a student, especially where these may be uploaded to a Trust website.
- Images should not be of any compromising positions or in inappropriate clothing.
- Any photographs taken and used by the Trust on the website or for other purposes will be in accordance with the photograph procedures issued in the induction packs.
- The sharing of images via weblogs, forums or any other means on-line will only occur after permission has been given by the parent/ Member of Staff.

10.Inappropriate Use

In the event of staff misuse

If an employee is believed to have misused the internet or Trust network in an illegal, inappropriate or abusive manner, a report must immediately be made to the appropriate leader depending upon where the alleged misuse occurred or by whom:

- On school / college site (including if by a member of staff from the central Trust team or from another establishment from within the Trust) – **Headteacher of the establishment**
- Off-site by a member of school / college staff – **Headteacher of their establishment**
- By a member of the central trust team either on central Trust property or off-site - **CEO**
- By the Headteacher or member of the Trust Leadership Team (CEO, CFO, COO) – **Chair of Trustees**
-

The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- Trusts Senior HR Advisory Team
- LADO (Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the e Safety Incident Flowchart within the accompanying Employee Handbook for further details.

In the event of minor or accidental misuse, internal investigations should be initiated, and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

- Accepting or requesting students as 'friends' on social networking sites or exchanging personal email addresses or mobile phone numbers with students.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

Inappropriate use by a child or young person

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. Template student Acceptable Use Rules and example sanctions can be found in the appendix.

Students should recognise the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with employees.

11. Policy Review

The Acceptable Use Policy will be updated to reflect any technological developments and changes to the Trust's ICT Infrastructure. Acceptable Use Rules for students should be consulted upon by the student body to ensure that all young people can understand and adhere to expectations for online behaviour.

12. Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting Trust Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/Trusts/pages_view.asp?did=9786

ACCEPTABLE USE POLICY (AUP): Staff agreement form

To be read in conjunction with the Staff Code of Conduct.

Covers use of digital technologies in Trust: i.e. email, Internet, Intranet and network resources, learning platform, software, equipment and systems.

- I will only use the Trust's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Committees of the Trust
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet/ Intranet / network or other Trust / LA systems.
- I will ensure all documents, data etc; are saved, accessed and deleted in accordance with the Trust's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any Trust business. (This is currently: Microsoft Outlook and Web access).
- I will only use the approved Trust email, Trust Learning Platform or other Trust approved communication systems with students or parents/carers, and only communicate with them on appropriate Trust business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/Trust name contact.
- I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive) to the network/Internet that does not have up to date anti-virus software and I will keep any 'loaned' equipment up to date, using the Trust's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission.

- I will use the Trust's Learning Platform in accordance with Trust protocols.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the Trust is provided solely to support my professional responsibilities and that I will notify the Trust of any 'significant personal use' as defined by HM Revenue & Customs.
- I will access Trust resources remotely (such as from home) only through the Trust approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow Trust data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the Trust's named Designated Safeguarding Lead if I feel the behaviour of any child / teacher may be a cause for concern.
- I understand that all Internet usage/and network usage can be logged, and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-Trust safeguarding approach and will report any behaviour (of other staff or students), which I believe may be inappropriate or concerning in any way, to a senior member of staff/named child protection officer at the Trust.
- I understand that failure to comply with this agreement could lead to disciplinary action.

ACCEPTABLE USE POLICY (AUP): Staff agreement form

User signature

I agree to abide by all the points above

I understand that it is my responsibility to ensure that I remain up to date and that I have read and understand the Trust's most recent e-safety and safeguarding policies.

I wish to have an email account; be connected to the Intranet and Internet and to be able to use the Trust's ICT resources and systems.

Signature _____ **Date** _____

Full Name _____ (printed)

Job Title _____

Trust _____

Authorised Signature (CEO/COO)

I approve this user to be set up

Signature _____ **Date** _____

Full Name _____ (printed)