Nene Education Trust

Acceptable Use Policy

Key Manager	**Governance Manager**
Ratified by Directors	
Review Dates	
Location of Policy	**Trust Intranet**
Access to Policy	**Open**
Policy Context	**This policy applies to all users of technology within the Nene Education Trust**

Revision History

Revision Date	Description	Sections Affected	Revised By	Approved By
July 2020	New policy	All	CBN	CHI
July 2023	Updated policy	All	DSm	

Nene Education Trust ("the Trust") is a multi academy trust and includes all the academics within it and is the employer of all staff within those academies.

The Trust is committed to creating a safe teaching and learning environment in its academies and offices and in order to do so, effective policies and procedures which are clearly understood and followed by the whole Trust community are essential. The Trust also recognises the impact that the effective and safe use of educational technology can have to enhance teaching and learning in the classroom, leading to enhanced educational outcomes, and the role of technology to improve effective and productive administrative functions. Our intention is that technology used across the Trust will enhance and not hinder the working practices of staff and students.

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 across the Trust. The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate developments with ICT.

The purpose of the Acceptable Use Policy is to clearly identify across the Trust:

- the steps taken to ensure the online safety of all users when using the IT systems in place, including, but not limited to the internet, online platforms and email.
- the Trust's expectations for the behaviour while using the internet, email and related technologies provided by the Trust.
- the Trust's expectations for the behaviour while accessing and using data owned by the Trust.
- the Trust's expectations for the personal conduct and behaviour of users accessing their own personal IT where this could have a negative impact on the Trust and it's ethos.

2. Scope of policy

The policy applies to all pupils, Trust employees, including individuals working in a voluntary capacity. All academies and Central Trust Office are expected to ensure that non-employees on site are made aware of the contents of this policy if they access the Academy/Trust IT services.

This Acceptable Use Policy should be used in conjunction with the Academy's Child Protection and Safeguarding Policy, the Trust's disciplinary procedures and code of conduct applicable to all employees and pupils. The Trust's Director of Operations~~Chief Executive Officer~~ (DOO~~CEO~~) will be responsible for its distribution and relevant senior managers will be responsible for its implementation. Within a school setting the relevant manager is the Principal.~~its implementation~~.

3. 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.

This policy refers to, and complies with the following legislation and guidance:

- Data Protection Act 2019
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The telecommunications Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023~~18~~
- Searching, screening and confiscation: advice for schools
- The Waste Electrical and Electronic Equipment Regulations 2006 & 2007

4. Responsibilities

Trust

The Trust has the responsibility for the strategic direction of the ~~Trust's~~ IT Strategy while also monitoring and evaluating the use of associated IT strategies across Academies within the Trust. The Trust will:

- work with Academy designated leaders for IT to develop, implement and evaluate the Trust IT strategy.
- provide support, resources and time for IT leaders, e-Safety leads and safeguarding teams to ensure that agreed policies are implemented, staff trained and protocols followed.

Principal

The Principal of each Academy has the overall responsibility as the wider remit of safeguarding and child protection. To meet these responsibilities, the Principal should:

- m~~M~~onitor the implementation of this policy in their academy

- 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, pupils and volunteers should be aware of who holds this post within the academy.
- 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 Academy Improvement Plan.
- share any e-safety progress and curriculum updates at all local governance meetings and ensure that all present understand the link to child protection.
- ensure that e-safety is embedded within all child protection training, guidance and practices.
- elect a Safeguarding to challenge the academy about e-Safety issues.
- make employees aware of the Inter-agency Child Protection Procedures at http://www.northamptonshirescb.org.uk/

E-Safety Lead

Each Academy should nominate an e-Safety lead who should:

- recognise the importance of e-Safety and understand the Trust's/academy's duty of care for the safety of their pupils and employees.
- establish and maintain a safe ICT learning environment within the Trust/academy.
- ensure that all individuals in a position of trust who access technology with pupils 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/academy equipment.
- report issues of concern and update the Principal on a regular basis.
- liaise with the 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 a log of all e-Safety Incidents in 'My Concern' or an equivalent secure record
- with the support of the Network Manager or ICT Lead, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate (academies 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.
- Make use of Securly monitoring software to monitor the traffic going through their individual school's systems to identify and monitor key markers in the monitoring software

Individuals

All Trust employees, pupils and volunteers 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 Principal, including the unacceptable behaviour of other members of the Trust community.
- use Trust/academy ICT systems and resources for all Trust/academy related business and communications, particularly those involving special category pupil data or images of pupils. Trust/academy issued email addresses, laptops, mobile phones and cameras must always be used unless explicit permission has been agreed for the use of a personal device.

- ensure that all electronic communication with pupils, 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 pupils and their families (please refer to code of conduct with regard to contact with parents in our school community.)

- Employees and volunteers are personally responsible for what they communicate in social media and must bear in mind that what is published might be read by the colleagues, pupils, parents and carers, the general public, future employers and friends and family for a long time. Employees and volunteers must ensure that their on-line profiles are consistent with the professional image expected by the Trust and must not post material which damages the reputation of the Trust or which causes concern about their suitability to work with children and young people. Those who post material which may be considered as inappropriate could render themselves vulnerable to criticism or, in the case of an employee or volunteer, allegations of misconduct which may be dealt with under the **Disciplinary Procedure**. Even where it is made clear that the writer's views on such topics do not represent those of the Trust, such comments are inappropriate.

- Employees and volunteers are advised not to have any online friendships with any young people under the age of 18, unless they are family members or close family friends. Employees and volunteers are advised not to have online friendships with parents or carers of pupils, or members of the governing body/Trustees. Where such on-line friendships exist, employees and volunteers must ensure that appropriate professional boundaries are maintained.
- Employees should make careful consideration when joining WhatsApp or social networking groups related to their schools and their own children to ensure professional integrity and to allow them to maintain professional distance where appropriate.
- ~~.~~

~~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 lock screens when leaving workstations. All users should log-off the network wherever possible when leaving work stations unattended.
- understand that network activity and online communications on Trust/academy equipment (both within and outside of the Trust/academy environment) may be monitored through the Securly monitoring system. ~~.~~
- This includes but not limited to IP address, access times and any personal use of the Trust/academy network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out
- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

5. Unacceptable use

The following is considered unacceptable use of the Trust's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings

Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Using Smart watches, mobile phones or similar technology to record video or sound at any point while on school property~~during lessons.~~

- Using school equipment for personal use beyond what is required and acceptable for the role of the individual.
- Breaching the Trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the Trust, or risks bringing the school into disrepute
- Sharing confidential information about the Trust, its pupils, or other members of the school community
- Connecting any device to the Trust's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust
- Using websites or mechanisms to bypass the Trust's filtering mechanisms

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The CEO and or Principal will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

If there are any low level concerns in relation to the conduct of another member of trust staff please refer to the managing allegations policy.

~~Inappropriate use~~

~~Any action which contravenes the guidance outlined in the following pages.~~

~~Inappropriate use includes, but is not limited to any behaviour that makes use of Academy/Trust IT services in an illegal, inappropriate or abusive manner. Inappropriate online behaviour outside of the Academy/Trust IT services could also be deemed as of inappropriate use, for example accepting requests from pupils on social media or acting in a way that would lead to questions on an individual's suitability to work with children or act as a role model.~~

~~In the event of inappropriate use by staff a report must be made to the Principal, Designated Safeguarding Lead, CEO. The appropriate procedures for allegations should be followed as per the Trust's disciplinary procedures, including contact made to relevant local authorities.~~

~~In the event of inappropriate use by students the Academy's behaviour policies should be used to investigate and implement appropriate sanctions as a result. In the event of accidental access to inappropriate materials, pupils are expected to notify an adult immediately and attempt to close the content immediately. Pupils should be made aware of and 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.~~

6. Consent for use

On entry to the Academy or the Trust, consent is sought from staff and parents (on behalf of their children) for the use of ICT and images. All members of the Academy and Trust community will sign an Acceptable Use Agreement which covers the use of ICT equipment and services, images and film, including video conferencing.

Consent for images and film
Permission is sought from staff and parents (on behalf of their children) for:

- images and film to be used on the Academy or Trust's website, prospectus or other printed publications that the Academy may produce for promotional purposes.
- images and film to be transmitted and/or recorded on a video or webcam under controlled situations.
- images and film to be used in display material used in the Academy or Trust's communal areas or external areas promoting the Academy.
- images and film to be used in general media appearances or social media sharing the success of the Academy or Trust.

Consent is considered valid for the entire period of the staff's employment or the pupils time at the Academy unless there is a change in circumstances. Consent can be withdrawn at any time, in writing to the Principal. For children, all legal guardians must give approve the change of consent. Students full names will not be published alongside their images.

Images and film may be stored on the Academy network (each academy will determine where this is stored) and access will be controlled to only those who must have access, for example Website Managers or Senior Leaders. Access to these images will be directed by the Principal and stored in line with acceptable use agreements signed by parents. Please refer to the Trust's Data Retention Policy.

Webcams and CCTV
CCTV is used in some areas for security and safety. The only employees with permission to access recordings are the Site Manager, Office Manager and the Senior Leadership Team. Notification of CCTV use must be displayed at the front of the Academy.

Public webcams are only used in the Academy where they are for a specific learning purpose, for example, in a class experiment, pupils may be monitoring hens' eggs. Misuse of this facility will be classed as inappropriate use and the relevant procedures applied.

Video conferencing
From time to time, there may be a benefit of completing a video conference to enhance or embed learning. Where pupils are involved in these opportunities they will be supervised by a member of staff when conferencing with users from outside the Academy. The Academy will keep a record of conferences of this form, including date, time and participants. Approval for opportunities involving users from outside the academy~~of this form~~ should be sought from the Principal before taking place.

7. Use of Trust and personal ICT equipment

The Trust manages access to ICT facilities and materials for users including, but not limited to:

- computers, tablets and other devices
- access permissions for certain programmes
- access to the Trust Office365 tenancy

In order to prevent infection of Trust equipment with viruses:

- all files downloaded from the Internet, received via email or stored on removable media should be checked for any viruses using Academy provided anti-virus software before their use.
- individuals should never interfere with any anti-virus software installed on Academy ICT equipment.
- if individuals suspect there may be a virus on Academy ICT equipment they should stop using it and contact the relevant IT Support staff immediately
- ~~The use of portable memory devices is not approved.~~
  - ~~Are all devices encrypted including laptops? And can guidance be issued on a secure password.~~

An inventory of all Academy and Trust IT equipment is kept by each Academy's IT Support team and records of allocations of devices to individuals is kept. Users should avoid not leave any portable or mobile ICT equipment unattended in vehicles. Where this is not possible they should be locked out of sight. Users who are allocated Trust ICT equipment are responsible for its security at all times. Upon leaving the Academy all equipment must be returned along with a list of all user accounts so that these can be disabled.

Employees must be aware that while personal equipment is being used for academy purposes it is still open to monitoring through the trust Securly network management once signed in through a trust account such as Outlook following the download of the SSL certificate to allow use of the device.

The use of removable media such as CDs, flash drives or portable hard drives is prohibited. Where possible, these media will be disabled by the Academy IT support teams. If media of this form must be used, permission should be gained from the Principal or the designated Senior Leader with responsibility for IT.

Personal devices should only be connected to the school network with prior authorisation from the Principal or the Senior Leader with delegated responsibility for IT. (Appendix 4)

When using Trust or Academy services away from school staff or students may use personal devices, for example to access Office365 services. This is deemed as 'remote access' (see section 14 for more information). When using personal devices users are responsible for the security of their devices and should apply the same processes and protocols they would on site. Users must:

- take appropriate actions to ensure that devices are protected against malware including viruses.
- take appropriate actions to ensure that devices are secure and protected by passwords and/or other encryption methods.
- not download or save sensitive or confidential data onto personal devices outside of Trust provided storage such as Office365.
- Delete temporary download files on their computer

Users should be aware that when they access school services such as Office365 via personal devices, associated data can be wiped remotely by removing access to these files and services following the departure of the user from the trust, or in the event of a security breach.

Mobile phones

The Academy and Trust allow staff, and in some cases, pupils, to bring personal mobile phones onto the site for their own use. Under no circumstances should a member of staff contact a student or parent/carer with their own personal device without express permission from the Principal.

The Academy is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate messages between any members of the Academy community is not allowed. Permission from the Principal must be sought before the capture of any image, film or audio recording using personal mobile phones. Users bringing personal devices onto the Academy site must ensure that there is no inappropriate or illegal content on the device.

The Trust and/or Academy may provide a Trust owned mobile phone to some staff or Senior Leaders. These devices are treated and monitored in the same fashion as other IT equipment and must be treated as such.

The Trust has a separate policy regarding the safe use of mobiles and cameras. This includes: Personal devices are only to be used by staff when on a designated break away from the pupils. At all other times, personal devices are to be switched off.

Trust and or Academy devices are only to be used by staff for work purposes. Photographs and videos of the pupils are only to be taken on school devices.

Images of the pupils will only be used in accordance with our Data Protection Policy.

Servers

Across the Trust and Academy network there are a number of servers used to store data and provide network services. In all cases, servers:

- are kept secure in a locked environment.
- have limited access rights to only those that need them.
- are backed up at regular intervals and encrypted, as advised by the IT Support team.
- have archived copies of secure data retained for the necessary timeframes in accordance with the Trust's data retention policy.

Telephone systems

Staff users may make or receive telephone calls as part of their employment at the Academy and or Trust. Users should be aware that the laws of slander apply to telephone calls and while the call may be temporary, use in this way will be deemed as inappropriate use and the ~~Academy's~~ Trust's disciplinary processes followed.

8. User security

The Trust and Academy gives individuals access to its IT systems and services, including for staff to Management Information Systems. All of these services are accessed with a unique ID and password. It is the responsibilities of all users to keep passwords secure. Individual users are responsible for all activity on ~~Academy~~ Trust and academy systems regardless of the device being used to access services.

- Passwords will be provided by the ~~Academy~~ Trust and must be reset by users on first logon.
- Individuals must not share their user ID or password with other users.
- Complexity requirements are set by the IT Support teams and are age and role appropriate.
- Individuals are advised not to include passwords in any automated logon procedures.
- Individuals are advised not to record passwords or encryption keys on paper or in unprotected files.

If an individual thinks their password may be compromised or are aware that another user has access to someone else's password this should be reported to the ICT support team.

S~~enior s~~taff across the Trust and Academies, will~~or those with access to significant amounts of confidential data may~~ be expected to use further security measures such as two factor authentication to prevent unauthorised access this will use Microsoft Azure as an access app and will allow users to securely access Trust apps on any device safely. ~~.~~

9. Internet use

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use is logged through Securly and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

In accessing the Internet, everyone~~individuals~~ must:

- overserve software and content copyright at all times. It is illegal to copy or distribute software or content to other sources.
- not share personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience especially on social networking.
- reveal the names of colleagues or pupils, or any other confidential information acquired through your job on any social networking.
- under any circumstances use the Internet to access online gaming, gambling or content of any nature that is illegal or could cause offence, including, but not limited to pornographic, racist, sexist or homophobic content.
- not download programs or files on Academy ICT equipment without seeking prior permission from the Principal or designated Leader with responsibility for IT.
- be cautious in the use of the information given by others on sites to take account of bias and accuracy of information.
- not access personal social networking on ~~Academy~~ Trust ICT equipment.
- avoid placing images of themselves, or details within images that could give details, on social networking or other Internet sites that could lead to further risk or danger.
- avoid sharing personal data over the Internet which may identify themselves or others and lead to further risk or danger.
- set and maintain privacy options where they are available to protect themselves and others.
- encouraged to be wary about publishing specific and detailed private thoughts online.
- report any incidents of online bullying to a member of staff or a line manager.
- follow guidance for the use of online interactions between pupils and staff, as directed by the Principal or Senior Leader responsible for IT.

The Trust/Academy will support the safe use of the Internet by:

- supervising access to Internet resources (where reasonable) to minimise risk.
- recommending useful sites for students before use.
- discouraging raw image searches when working with students.
- suggesting specific sites for home based research tasks.
- controlling and monitoring the sites that can and cannot be accessed through adequate filtering using Securly web filtering
- Utilising 2 factor authentication and Microsoft Azure to limit access to specific sites~~.~~

10. ~~10. Email~~
Email

The use of email within the Trust and Academies is an essential method of communication for all users. In the context of the Trust, individuals should not consider emails to be a private method of communication. Members of trust staff need to also avoid having emails and messaging apps on screen~~open~~ during teaching times to prevent interruptions and sensitive information being on show to students and to avoid GDPR breaches.

~~Each Academy~~The Trust gives all staff their own email account as a tool for all Academy business. Personal email accounts must not be used for this purpose. Pupils will be given email accounts under the discretion of each Principal who will make a judgment on the age appropriateness of their use.

It is the responsibility of the individual to manage their own accounts by:

- keeping their email password secure.
- carefully checking all emails before sending, in the same was as a letter written on Academy or Trust headed paper.
- deleting all emails of short term value and organising their inbox to support later searching.
- not sending chain mail within the Trust/Academy email system.
- keeping the number and relevance of email recipients, particularly those being copied in, to a minimum of necessary and appropriate users.
- avoid sending attachments unnecessarily, instead using shared documents or files available on the system.
- not using the academy email for personal reasons.
- only using their provided email account for Trust or Academy related business.
- checking their email regularly when appropriate to do so.
- activating "out of office" notifications when away for extended periods.
- never opening attachments from untrusted sources. In this scenario, support should be requested from the IT Support services.

Individuals must be aware that:

- the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- if an email is received in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- if an email is sent in error which contains the personal information of another person, they must inform the Data Protection Officer, Principal and Governance Manager immediately and follow the data breach procedure.

The Trust~~/Academy~~ will support the safe use of email by:

- logging all emails so that inappropriate emails can be traced if necessary.
- implementing a standard disclaimer that is attached to all email correspondence to state that "the views expressed in this email are not necessarily those of the Academy or the Trust".
- managing the email system to ensure that it is secure and safe for users at all times.

The Trust recognises that pupils need to understand how to style an email in relation to their age and good email etiquette. Academies will develop students email confidence through ICT lessons.

Personal use

Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The [network manager/ICT manager/SBM/headteacher/etc.] may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during [contact time/teaching hours/non-break time]
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust's [mobile phone/personal device policy].

Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the Trust's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The Trust has guidelines for staff on appropriate security settings for Facebook accounts.

11. Personal, sensitive and confidential information and Data Protection

Individuals must keep all ~~Academy~~ Trust related data secure. This includes all personal, sensitive, confidential and classified data. It is the responsibility of the individual to ensure the security of this data. To do this, individuals must:

- ensure that any ~~Academy~~ Trust information accessed from personal devices (only when approved) is kept secure through relevant user security and anti-virus.
- ensure that devices are locked before moving away from workstations to prevent unauthorised access to others.
- ensure the accuracy of any data that is being shared or disclosed with others.
- only download personal data from systems if expressly authorised to do so.
- must not post on the Internet any information or data in any way that may compromise its intended restricted audience.
- keep their screen display out of direct view of any third parties when accessing data of this nature.
- ensure hard copies of data are stored securely and disposed of after use in accordance with the document labelling.

Emailing personal, sensitive, confidential and classified information

From time to time it may be necessary to send an email containing sensitive information. On these occasions the individual sending the email must:

- consider whether the information can be sent by any other secure means such as access to a shared area or secure transmission service.
- where the conclusion is that email must be used to transmit data:
    - obtain express consent from their line manager to provide the information by email

- verify (at least by email and phone) the recipients details prior to sending the data
- the email must not be copied or forwarded to any more recipients than absolutely necessary.
- use a secure email system such as egress or encryption via Office365 where possible.
- the information should be encrypted documents attached to the email with the encryption key password provided in a separate communication to the recipient(s).
- not identify the information in the subject line of the email.
- request confirmation of safe receipt.
- If a file is attached to an email containing personal information, it must be password protected and sent separately when requested.

Safe use of images

Digital images and film are increasingly easy to capture, reproduce and publish, and as a result therefore misuse. We must remember that is not always appropriate to take or store images of any member of the ~~Academy~~ Trust community or public, without first seeking consent and considering appropriateness.

The written consent of parents (on behalf of students) and staff will be collected on entry to the Academy. With this consent the Academy permits the appropriate capture of images and film by staff and students using Academy equipment.

Staff are not permitted to use personal equipment, such as mobile phones and cameras to record images of students without the express permission of the Principal.

Students are not permitted to use personal equipment to record images of others.

12. Remote access using a personal device

Academies may use a remote access system. Remote access is deemed as any form of accessing school IT services from a device that is not owned by the Trust ~~or Academy~~. This includes the use of personal ~~mobile~~ devices to access emails and files. It is the responsibility of individuals for all activity that is carried out using their remote access credentials. Individuals should:

- only use equipment with appropriate security in place, including anti-virus and user security.
- prevent unauthorised access to ~~Academy~~ Trust systems by keeping their access credentials secure at all times.
- protect ~~Academy~~ Trust information and data at all times, including any printed material produced while using the facilities.
- take particular care for data security when access is from a non-Academy environment.
- report any breaches in data in line with expectations of the Trust Data Protection policy. This includes breaches where an associated user has accessed services on a Trust or personal device away from school or in the case of theft/loss of a device that has been used to access Trust IT services.
- remember that when accessing systems remotely, they must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Trust's ICT facilities outside the Trust.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

13. Equal opportunities

The Trust ~~and Academy~~ endeavours to create a consistent message with ~~parents for all students~~users across all areas of its business. Some users may require additional training and

teaching including reminders and prompts to reinforce their existing knowledge and understanding of both technical and safety issues. Where a user needs further support, particularly regarding safety, careful consideration must be given to group interactions when raising awareness of safety. Internet activities are planned and well managed carefully for these users.

14. Parental involvement

The Trust and Academies believe it is essential for parents/carers to be fully involved with all aspects of children's education, especially promoting online safety practices both in and outside of the Academy. Academies will regularly consult and discuss online safety with parents/carers and seek to promote a wider understanding of the benefits related to ICT and associated risks.

Parents/carers are:

- actively encouraged to contribute to adjustments or reviews of the Academy online safety policy
- asked to read through and sign the acceptable use agreements with their children on admission to the Academy
- required to make a decision as to whether they consent to images of their child being taken and/or used in the public domain, for example the Academy or Trust websites or social media.
- expected to support the Academy's approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the Academy community.

The Trust and Academy will disseminate information to parents relating to online safety in the form of information and celebration evenings, posters and websites, newsletter items and social media.

15. Dormant accounts

Dormant accounts (sometimes referred to as zombie accounts) are those where the users have left the ~~Academy~~ Trust and therefore no longer have authorised access to the ~~Academy or~~ Trust's systems. The IT Support team in each Academy have the responsibility to ensure that user accounts remain up to date and disable accounts once the user has left the ~~Academy~~Trust.

To support this process, generic passwords shared by users, for example, to access an online teaching resource, should be changed regularly to avoid unauthorised access. It is advised this is done at least once per academic year, or for higher security once per term.

16. Disposal of redundant ICT equipment

Redundant ICT equipment will be disposed of through an authorised agency. During this process:

- all Trust data will be deleted by the IT Support services to ensure that data is irretrievable in the future. Where the IT Support services are not confident that the data is irretrievable the physical media will be destroyed internally.
- upon collection of the equipment the authorised agency must provide a receipt that confirms their acceptance of responsibility for the destruction of the equipment including a certificate of data destruction to NCSC standards.

In order to support this process each Academy's IT Support service will build and maintain a comprehensive inventory of all its ICT equipment, recording information relating to disposals:

- date item was disposed
- Senior Leader authorisation of disposal
- verification of licensing
- record of how it was disposed

. Monitoring and review

The headteacher and [ICT manager/network manager/SBM/etc.] monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the Trust.

This policy will be reviewed every [number] years.

Acceptable Use Policy

Appendix 1

Condensed Acceptable Use Agreement for Primary age students~~students~~

As part of our curriculum students across Academies within the Nene Education Trust will be accessing computers, the internet and when appropriate Office365 services. Across the Nene Education Trust we take the safety of students very seriously and as such are only allowing students access to these resources once completed acceptable use agreements have been received. In the event of a breach of the rules by any child or young person the relevant Academy will take action in line with the acceptable use policy and the respective behaviour policy.

Students are taught about the importance of e-safety and their actions online as part of the curriculum and we would encourage parents/carers to continue these conversations about the safe and appropriate use of the internet and other online tools, including social media, both within and beyond school.

Child's name: .....

Child's date of birth: .....

Child's school: .....~~I must respect copyrights and trademarks and not publish or submit work that is not my own.~~
~~I must only open attachments and downloads from users I know and trust.~~
I agree to be responsible and sensible in my use of all ICT resources school

- I understand that I am responsible for my own behaviour.
- I will log out of my device when it is no longer being used.
- I will keep my username and password private and not share it with others.
- I will not purposely access, create or display any material that may upset others.
- I will not share personal information about myself, or anyone else.
- I will not knowingly access any inappropriate/age related content.
- I will not respond to negative or inappropriate email messages – I will report them to a trusted adult.
- I will make sure that I speak to a trusted adult should I find something that concerns or worries me.

I understand that my school uses a monitoring and filtering system called Securly and understand that my use of ICT on my school account can be checked both in and outside of school.

I know that any failure to follow the contents of the acceptable use policy will result in the partial, or full, temporary or permanent loss of access to services and further action may be taken in line with the Academy's behaviour policy where necessary.

Signed (child): .....

Date: ……

[Note: The Academy will whether or not they wish the children to sign the agreement, and at which age, for younger children the signature of a parent/carer is sufficient]

Parent declaration

I have read and discussed the guidance above with my child to ensure that he/she understands the importance of the acceptable use agreement and staying safe using technology.

I confirm that I understand that the school will provide access to age appropriate technology and use appropriate measures including supervision, filtering and monitoring is in place.

I understand that unfortunately, despite all protective measures, inappropriate materials may be accessed. Where this happens accidentally the Trust/Academy will follow the acceptable use policy and handle this as necessary. Intentional access to this material by my child will be deemed as a breach of the acceptable use agreement and will be handled in accordance with the policy and the Academy's behaviour policy.

I understand that whilst my child is using the internet or other tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Signed (parent/carer): ……..

Name (parent/carer): ……..

Date: ……

Acceptable use policy
Appendix 1.1

Condensed Acceptable Use Agreement for Secondary age students

As part of our curriculum students across Academies within the Nene Education Trust will be accessing computers, the internet and when appropriate Office365 services. Across the Nene Education Trust we take the safety of students very seriously and as such are only allowing students access to these resources once completed acceptable use agreements have been received. In
the event of a breach of the rules by any child or young person the relevant Academy will take action in line with the acceptable use policy and the respective behaviour policy.

Students are taught about the importance of e-safety and their actions online as part of the curriculum and we would encourage parents/carers to continue these conversations about the safe and appropriate use of the internet and other online tools, including social media, both within and beyond school.

Do we not need a statement in here about mobile phone and smart watches so each student signs up to the agreed use of such?

Child's name: .....

Child's date of birth: .....

Child's school: .....

Student Acceptable use of ICT

~~**I agree to be responsible and sensible in my use of all ICT resources school**~~

- ~~*I understand that I am responsible for my own behaviour.*~~
- ~~*I will log out of my device when it is no longer being used.*~~
- ~~*I will keep my username and password private and not share it with others.*~~
- ~~*I will not purposely access, create or display any material that may upset others.*~~
- ~~*I will not share personal information about myself, or anyone else.*~~
- ~~*I will not knowingly access any inappropriate/age related content.*~~
- ~~*I will not respond to negative or inappropriate email messages – I will report them to a trusted adult.*~~
- ~~*I will make sure that I speak to a trusted adult should I find something that concerns or worries me.*~~

~~*I understand that my mobile phone should be turned off and away during lessons and that smart watches are to be disconnected and used as a watch during these periods*~~

I understand that at no times during lessons I should take any type of video on any personal device.

I agree to be ready, responsible and respectful in my use of ICT resources, including the use of hardware devices, software packages, Microsoft Teams/Office365 and the internet.

- I understand that I am responsible for my own behaviour.
- I will lock my computer screen if I leave my workspace.
- I will keep my username and password private and regularly update it when prompted.
- I will not purposely access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to others, such as bad language racist, sexist, abusive, homophobic or aggressive words.
- I will not share personal information about myself, or anyone else.
- I will avoid accessing any inappropriate/age related content.
- I will not respond to negative or inappropriate email messages – I will report them instead.
-

By pressing CTRL+ALT+DEL to log in, I accept the points stated above.
I understand that my school uses a monitoring and filtering system called Securly and understand that my use of ICT on my school account can be checked both in and outside of school.

I understand that Manor school uses the Smoothwall monitoring and filtering system and I may be questioned about my internet use and/or the use of others that I may have witnessed.

By pressing CTRL+ALT+DEL to log in, I accept the points stated above.
I understand that my school uses a monitoring and filtering system called Securly and understand that my use of ICT on my school account can be checked both in and outside of school.

I know that any failure to follow the contents of the acceptable use policy will result in the partial, or full, temporary or permanent loss of access to services and further action may be taken in line with the Academy's behaviour policy where necessary.

Signed (child): .....

Date: .....

[Note: The Academy will whether or not they wish the children to sign the agreement, and at which age, for younger children the signature of a parent/carer is sufficient]

Parent declaration

I have read and discussed the guidance above with my child to ensure that he/she understands the importance of the acceptable use agreement and staying safe using technology.

I confirm that I understand that the school will provide access to age appropriate technology and use appropriate measures including supervision, filtering and monitoring is in place.

I understand that unfortunately, despite all protective measures, inappropriate materials may be accessed. Where this happens accidentally the Trust/Academy will follow the acceptable use policy and handle this as necessary. Intentional access to this material by my child will be deemed as a breach of the acceptable use agreement and will be handled in accordance with the policy and the Academy's behaviour policy.

I understand that whilst my child is using the internet or other tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Signed (parent/carer): .....

Name (parent/carer): .....

Date: .....

Acceptable Use Policy

Appendix 2

Condensed Acceptable Use Agreement for **Staff, Volunteers and other Adults**

Staff name: ……..

To ensure that all adults within the Nene Education Trust are aware of their responsibilities when accessing any Academy IT equipment or online services, they are asked to sign this Acceptable User Agreement. This is to ensure that adults role model the safe and responsible use of these technologies for students as well as inform and protect users so that they feel safeguarded and avoid inadvertent misuse themselves.

I have read and understood the acceptable use policy. In particular, I understand/know:

- I must only use Academy/Trust equipment in an appropriate manner and for professional use as per the acceptable use policy.
- I am familiar with the Trust disciplinary procedures so that I can deal with any incidents of misuse that may arise.
- I am responsible for reporting any accidental misuse in line with the acceptable use policy.
- I must report any incidents of concern for a child or young person's safety to the Principal, Designated Safeguarding Lead or e-Safety Lead in accordance with the safeguarding policies in place in each academy.
- who the Designated Safeguarding Lead(s) is/are in my setting.
- I am putting myself at risk of misinterpretation and allegation if I contact other members of the school community, via personal technologies. In particular, I must not contact students or parents/carers in any way other than the Trust/Academy designated communication systems.
- I should only use the Trust/Academy provided equipment and services for Trust/Academy related business.
- I must take all reasonable actions to protect the confidentiality and security of Trust/Academy equipment and data in accordance with the acceptable use policy, the Data Protection Act 1998, GDPR regulations and the Staff Code of Conduct.
- that I am responsible for all user activity completed with my accounts and as such must keep usernames and passwords secure at all times.

Signed ……..……..

Date: ……

Nene Education Trust

Acceptable Use Policy

Appendix 3

Trust/Academy IT equipment issuing agreement

Staff name: ……..

Academy name: ……

Device category/make/model:
……

Serial number: ……

The named member of staff has been issued with the device identified above by the named Academy. The member of staff is now the designated user and as such is responsible for its safe keeping and appropriate use.

The designated user must take appropriate measures to ensure the security of the device and any data stored upon it.

The designated user must use the device in accordance with the acceptable use policy and in line with guidance issued by Senior Leaders or the Academy's IT Support team.

The device remains the property of the Academy named and as such should only be used for Academy/Trust related business, not as a personal device.

By signing this agreement I assume full responsibility, including financial responsibility, for the device I take away from the Academy/Trust premises.

I certify by signing this form that I have current personal homeowners or renters insurance that contains coverage for the full replacement cost of this laptop device in the event of loss/theft.

If the loss / damage is not covered by insurance I agree to assume full financial responsibility and compensate the named Academy for the full replacement value for the device.

Signed ……..……..

Date: ……

Received by: ……..…….. (ICT Support)

Appendix 4

Use of personal device agreement

Employee/volunteer name: ……..

Academy name: ……

The use of a personal device relates to a personal device brought into the workplace as well as any personal device used outside the workplace, including at home. 'Employee' means employed member of staff or volunteer e.g. Trustee/Governor or similar

Do you intend to use a personal device for any work related matters YES/NO

Please indicate which work related aspects this device is used for:

- **Accessing email and Office 365 services**
- **Communication with colleagues**
- **Work related social media**
- **Use of school approved apps**
- **Use of online resources**
- **Other**

……..

Overview

- The employee or volunteer must take appropriate measures to ensure the security of the device and any data stored upon it.
- The device is the employee's property and remains the property of the employee at all times.
- The employee or volunteer must use the device in accordance with the acceptable use policy and in line with guidance issued by Senior Leaders or the Academy's IT Support team.

Security

- The device can be checked by the IT department to ensure that there are no security risks before it is used to access company data and information.
- The device should have virus protection installed.
- The security of company information and data is paramount. Employees must not do anything which might compromise that security when using their own devices.
- The device must be password-protected. The employee should not share the password with anyone without his/her line manager's knowledge and permission.

- The device should be set to lock when it is not in use.
- The device should not be used to access company data or information in a public place where non-employees might be able to see the content.
- The employee should never use the device to access company data over an unsecured network.
- The employee should ensure that there is a regular back-up of any company material that is placed on the device.
- If the device is lost or stolen, the employee must inform the line manager immediately, and always within 24 hours. It might be necessary for the IT department to remotely wipe the device clean. If this does happen there is no guarantee that personal information will not be deleted. A system should be in place to revoke access that a employee or volunteer might gain to a device in the event of loss or theft.
- If the device has a camera or video function, this must never be used in the workplace without the express permission of the employee's line manager and the consent of all the individuals who are being filmed.
- The following special category data and information must never be downloaded/stored on a personal device:
    - Student, parent and staff personal information. Employee personnel files.
    - Payroll reports.

Personal Use in the Workplace

- Although it is acknowledged that the device is the employee's personal property, employees must not spend time at work using the device for personal reasons. During working hours the device should only be used for company purposes.
- The personal device can be used for personal purposes during any designated breaks.
- Any personal device which is used for company purposes must never (during or outside working time) be used to access pornography or any illicit or illegal material.
- Personal calls should only be taken during working hours when the matter is urgent or an emergency.
- Unless the device has a hands-free facility, it should never be used when driving a motor vehicles.

Leaving the Organisation

- When an employee leaves the organisation, he or she must ensure that any company information has been removed from the device.
- The device can be taken to the IT department who will check the device to ensure that all company information has been removed.
- When a device is no longer being used, all company data and information must be deleted from the device. The IT department could be asked to check that this has been carried out thoroughly. Employees must ensure that when information is deleted, this is a permanent deletion, rather than being left in the device's trash system.

Breach of this Policy

Any breach of this policy could lead to disciplinary or legal action being taken against the employee concerned.

By signing this agreement I assume full responsibility for the compliant use of my personal device.

Signed ……..……..

Date: ……

Approved by: ……..…….. (Principal/COO/CEO)