# The Thomas Adams School

## Policy Statement

## ICT E-mail, Internet Use, ICT Security and Access Policy

Updated September 2021 □

Reviewed by Governors □

This policy applies to all school staff, students and third parties who use the school's ICT systems to access either e-mail or the internet.

# ICT E-mail, Internet Use, ICT Security and Access Policy

## 1 Rationale

The purpose of internet access in school is to enhance teaching and learning and to support the school's management information and business administration systems.

Access to the internet provides benefits in a wide range of areas, including teaching and learning resources, staff professional development, more efficient administration and rapid access via e-mail to a wide range of services provided by the council and between staff and students of the school.

Thomas Adams School has an ongoing commitment to invest significant levels of resources in the provision of ICT resources for students, staff and administrators of the school. These resources have become essential to the successful running and normal activities of the school.

The maintenance of these resources for all users and the protection of those users connected to the networks accessed by the school is therefore a responsibility that the school needs to meet.

## 2 Objectives

The objectives of this policy are to:

- Ensure the confidentiality and integrity of school information and assets.
- Ensure users are aware of and comply with, all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

## 3 Scope

For this Policy, information covers any method of information creation or collection, including electronic capture and storage, video and audio recordings, and any images, however created.

This Policy is intended for all school staff, including governors, who have control of or who use or support the school's administrative and/or curriculum ICT systems or data, or who handle other school electronic data.

The Policy will be reviewed on a regular basis.

Pupils using the school's ICT systems or data are covered by the rules governing internet and ICT use which are incorporated within this policy.

## 4 Responsibilities

### 4.1 The Owner

The Owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of the school. Exceptions to this are the software and documentation produced by individual teachers for lesson purposes. This includes schemes of work, lesson plans, worksheets or any other items agreed in writing by the Headteacher.

## 4.2 Role of the Governors

The Governing Body has the ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and information security and for disseminating policy on ICT security and other ICT related matters. In practice, the day to day responsibility for implementing these requirements rests with the Headteacher.

To also ensure that:

- All staff have access to all policy documents relating to this area
- All staff have the opportunity to comment on the policy
- The policy is reviewed as necessary

## 4.3 Role of the Headteacher

The Headteacher is responsible for ensuring that the legislative requirements relating to ICT systems and information security are met. The Headteacher is also responsible for ensuring that the Policy is updated on a regular basis to reflect changes in legislative requirements.

This responsibility includes ensuring that the requirements of the General Data Protection Regulation are fully complied with by the school and that staff are aware of both the provisions of this Policy and of the relevant legislation.

To also ensure that:

- All staff are given opportunities to discuss the issues associated with internet access
- All staff and students are aware that monitoring of internet access takes place and that privacy regarding internet access is not guaranteed or expected on the school systems.
- All staff are given access to this policy and are aware of its importance
- Internet activity is monitored as far as is practical and action taken as necessary
- Parents' attention is drawn to this policy and signposted to external safeguarding agencies eg CEOP.

## 4.4 The 3-18 Education Trust Manager

The Manager is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and defining and documenting the requisite level of protection.

The Manager will administer the practical aspects of ICT protection and ensure that, as far as is practical, data integrity, security copying, virus protection and network protection are all carried out. Additionally, the Manager will establish suitable rules for the physical access to systems and data.

In line with these responsibilities the Manager will be the official point of contact for ICT or information security issues and as such is responsible for maintaining a record of any breaches of ICT or information security. The record kept will additionally be used to notify the Headteacher or Chair of Governors of breaches of security.

The Headteacher or Chair of Governors must advise Internal Audit of any breach of ICT security or information security pertaining to financial irregularity.

## 4.5 Role of the staff

All users of the school's ICT systems and data must comply with the requirements of this Policy.

Users are responsible for notifying the Manager of any actual or suspected breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Local Governors Board or Internal Audit.

To also ensure that:

- Rules for internet access are posted near computer rooms;
- There is equality of access within the classroom;
- They inform ICT support department of any problems that arise;

## 4.6 Role of the students

- To read and understand the Acceptable Use Policy (see appendix A)
- To access the internet in a sensible manner
- To report to their teacher any material which they receive that they consider offensive or inappropriate
- To refrain from giving any personal contact details to any third party without the consent of their teacher.

## 5 Equal Opportunities

Opportunities should be provided for all students and staff to access the internet regardless of their gender, race, ethnic group, culture or ability.

## 6 Resources

It is expected that resources will be used from the internet for teaching and learning materials. Copyright must be acknowledged where necessary.

## 7 The Internet in the Curriculum

### 7.1 Teaching and Learning strategies

Internet access will be planned to enrich and extend learning activities. Pupils will be given clear objectives for internet use. Pupils will be guided to take responsibility for internet access by selecting appropriate sites and rejecting sites containing inappropriate material.

Pupils will be taught to:

- Validate information before accepting its is accurate
- Compare the internet with other media
- Determine when an internet resource is more appropriate than other resources such as books, papers, personal research
- To acknowledge sources of information by indicating the internet locations used
- Be aware that it is not always possible to identify the person sending an e-mail or creating a web page accurately
- Inform a teacher when faced with material they feel is inappropriate or offensive

### E-mail

Pupils need to be taught about the nature and content of e-mail and the ways this can differ from other forms of communication.

E-mail in the school is regarded as public and can be monitored. There is no expectation of privacy.

Pupils will be taught that they have responsibility for any e-mails sent from their address and should therefore keep all passwords and usernames secure and confidential.

Staff are reminded that for their own protection they should only use the school provided email systems for communication with pupils and parents so that an audit trail can be maintained. Use of other systems may leave members of staff open to allegations of misconduct. This also applies to the use of other systems such as Skype, Whatsapp and social media messaging services.

## Social Networking sites on the internet (see also Social Networking Policy)

Staff should be aware that information that they publish on any site on the internet, including social networking sites, could possibly be seen by pupils, parents and other stakeholders in the school. Care should be taken to set privacy settings on sites appropriately and to avoid publishing material that could cause embarrassment to the member of staff concerned or to the school (this could include comments or images about the school, pupils or personal activities).

Pupils, parents and other stakeholders should not be added as 'friends' to social networking sites and messaging services such as Whatsapp.

It should be noted that the publishing of inappropriate material could result in disciplinary action against the member of staff concerned. If a member of staff is uncertain whether particular material is appropriate they should seek guidance from the headteacher.

## Web and School controlled Social Media Publishing

The school website and school controlled social media has been designed to provide information about the school and to provide opportunities to disseminate information to parents. All public communication to parents and routine notices will be made available on the web site.

As the sites can be accessed by any computer outside the school the security of staff and pupils is paramount. The publishing of names beside photographs that identify individuals is acceptable with parental permission and compliance with GDPR. But remember some students should not be identified at all. If in doubt, please see Belinda Howells. Personal information or contact details must not be published without written consent.

Please note:

- The Headteacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained;
- Pupils will be made aware that the quality of their work published on the web should relate to the appropriate audience
- All material must meet copyright legislation
- The point of contact on the web site will be the school address and telephone number. Personal information and e-mail addresses will not be published
- Group shots or pictures taken over the shoulder will be used in preference to individual images;
- Permission from pupils and their parents will be sought before any personal data eg photographs of pupils, are published on the school web site.

## Microsoft Teams

Microsoft Teams is to facilitate the sharing of files, class communications and video conferencing. It should be treated as a school workspace and therefore complies with school behaviour and discipline policy. As it is used for setting homework, it also complies with the homework policy.

Teachers and staff will ensure that:

- They are professional with their interactions with staff and students
- They do not upload inappropriate, illegal and/or copyrighted material
- They avoid publishing material that could cause embarrassment to a member of staff, student or to the school
- Video chats and calls are used professionally and not one-to-one with students
- They comply with other school policies, whether in school or external

Student will ensure that:

- They are professional with their interactions with staff and students
- They do not upload inappropriate, illegal and/or copyrighted material
- They avoid publishing material that could cause embarrassment to a member of staff, student or to the school
- They do not start video chats and calls
- They comply with other school policies whether in school or external
- They do not interact with external people unless instructed to by a member of staff, and not one-to-one

As the platform can be accessed by any computer outside the school the security of staff and pupils is paramount. The publishing of names beside photographs that identify individuals is acceptable with parental permission and compliance with GDPR. But remember some students should not be identified at all. If in doubt, please see the Headteacher's PA. Personal information or contact details must not be published without written consent.

## **8 Internet Access**

Authorised users are given a unique username and password generated by the Manager. Individual users are responsible for their own password security. Users should not give their personal account details to any other user accept at the discretion of the Manager.

Filtering software is used to remove or alter pages of unsuitable content according to content filters set by default or custom lists. These lists are updated frequently via a 3rd party and reviewed internally upon request. No system can be completely effective and several approaches are used to support appropriate access to the internet. Final responsibility for material accessed however resides with the user.

All users must seek permission to download, distribute and use copy protected data. Any breach of copy protected data

Pupils and staff will be informed that their use of the internet will be monitored. Acceptance of filtering and monitoring is accepted upon use of the network.

Staff personal devices cannot be guaranteed access to the wireless network and should not join the wired network. Internet usage on personal devices must be limited, not to impact on the wider network. Appropriate anti-virus and firewall protection must be enable (if applicable).
All devices joined to the wireless network thus gaining access to the internet is at the discretion of the ICT manager.

**Access to inappropriate images and internet usage**

There are no circumstances that will justify adults possessing indecent images of children. Staff and students who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

Users should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Where other unsuitable material is found, including information or images covered on the 'Prevent' agenda (Radicalisation, Terrorism and Extremism) which may not be illegal but which raises concerns about that member of staff, the Local Authority Designated Officer (LADO) should be informed and advice sought. The school should not attempt to investigate or evaluate the material themselves until such advice is received.

## 9 Cyberbullying

The School's definition of cyberbullying is **'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'**

In order to reduce the potential for cyberbullying children must have their phones switched off when in school and put 'out of sight, out of mind'.

Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Staff are encouraged to report all incidents of cyberbullying to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

## 10 Legislation

### 10.1 Background

The major pieces of legislation relevant to this Policy are:

- General Data Protection Regulation 2018

- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988

All staff should be aware that infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

It should also be noted that other legislation may at times be relevant to this policy and the legislation above is not exhaustively listed.

Some of the general requirements arising from these acts are outlined below:

## **10.2 General Data Protection Regulation 2018**

This replaces the Data Protection Act 1998.
This requires the school to comply with its duties under the GDPR (2018).
Staff and governors should have due regard to the 6 principles of the Act. Data should be:
a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and 2
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

## **10.3 Computer Misuse Act 1990**

Under this Act the following are criminal offences, if undertaken intentionally:

- Unauthorised access to a computer system or data
- Unauthorised access preparatory to another criminal action
- Unauthorised modification of a computer system or data.

## **10.4 Copyright, Designs and Patents Act 1988**

This Act provides for the protection of intellectual property of the author of a piece of work. This includes computer programs and data.

Where computer programs are obtained from an external source they remain the property of the originator and permission is given to use these in the form of a contract or license.

The IT Manager is responsible for compiling and maintaining an inventory of all software held by the school and for checking the inventory's accuracy on a regular basis. To ensure that the school complies with the Copyright, Designs and Patents Act 1988 and in order to satisfy the 3-18

Education Trust's responsibilities as a corporate member of the Federation Against Software Theft, users must get prior permission in writing from the IT Manager before copying any software either to or from the school's ICT systems.

All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

## **11 Security**

### 11.1 Internet

The school put in place mechanisms to make internet access as safe as possible.  Staff will take all reasonable precautions to ensure that internet use is suitable for the age and maturity of the pupils concerned. However, as it is not possible to guarantee that inappropriate material will not appear on a computer screens the school cannot accept liability for material accessed or any consequences thereof.

Security of the school ICT systems is maintained by the following methods:

- Appropriate security strategies as advised by the IT Manager are implemented where appropriate for the school
- Virus protection and firewall systems will be implemented and updated regularly
- Internet filter
- Wireless controller policies
- Firewall filter
- Software updates will be applied regularly
- Hardware brought into the school will not be permitted on the school systems without specific authorisation and virus checking

### 11.1 Physical

Adequate consideration should be given to the physical security of rooms containing sensitive information and ICT equipment.  As far as practical only authorised persons should be allowed access to rooms that contain servers or provide access to data.

## **12  System Security**

### **12.1  Legitimate Use**

The school's ICT facilities must not be used in any way that breaks the law or standards detailed in the Education Department Personnel Guidance Manual.

### **12.2  Private Hardware and Software**

The use of all private hardware and software must be approved by the IT Manager prior to its being connected to the school networks.
The hardware and software should restrict or damage the network. It should also be used in a way that complies to the school's policies.
All private hardware and software is used at the owner's discretion and the school takes no responsibility for damage or breakages. The equipment will also not be covered by the school's insurance.
The hardware and software must also comply to copyright laws. The software must not interfere with the network, staff devices or external facing school resources.

### 12.3 ICT Security Facilities

The school's ICT systems and data must be protected by appropriate security measures as determined by the IT Manager.

### 12.4 Authorisation

Only persons authorised by the IT Manager, acting under the direction of the Headteacher, are allowed to use the school's ICT systems. The authority given to use the systems must not be exceeded and such authority should be reviewed regularly.

### 12.6 Passwords

The level of password control shall be determined by the IT Manager based on the value and sensitivity of the data involved.

Passwords and other forms of identification used to access the school's ICT systems should be kept confidential to the user and should be changed on a regular basis or if there is any suspicion that they may have been disclosed. Passwords should be memorised. If a password has to be written, this record must be stored securely.

### 12.7 Backups

The IT Manager should ensure that a suitable backup strategy is followed, having regard to the frequency of the backup, the potential for loss of sensitive data and the location of storage of backup media. Backup media and devices should be periodically tested for integrity.

### 12.8 Disposal of Waste

Disposal of waste ICT media should be made with due regard to the sensitivity of the information that they contain. This may involve shredding of paper or the incineration of other media.

### 12.9 Disposal of Equipment

The IT Manager should ensure that any personal or sensitive data is erased from school ICT equipment on its disposal or transfer from the school. The need for disposal extends to software stored on the equipment for which the school holds the licence.

When disposing of equipment the IT Manager must ensure that the requirements of the Waste from Electronic and Electrical Equipment (WEEEE) Directive are observed.

### 12.10 Repair of Equipment

If any equipment or its permanent storage is required to be replaced or repaired by a third party the significance of its data must be considered.

The school will ensure that third parties follow the General Data Protection Regulation, should the equipment store or contain personal data. This needs to be confirmed before the equipment is made available for repair.

## 13 Complaints/Problems

Complaints regarding internet use will be investigated as promptly as is practicable. The facts of each case will be determined and appropriate action taken. This may range from a reprimand for very minor transgressions of the policy to a ban on ICT access for a specified period of time. In a serious case it may be necessary to involve the local authority or the police.

- Any incidents should be reported to the ICT Manager in the first instance
- Pupils and parents will be informed of the complaints procedures
- A pupil may have access to the ICT systems denied for a period of time depending on the nature of the incident
- Denial of access could include all school work held on the system, including any examination or course work.

## 14 Management of the Policy

The Headteacher should allocate sufficient resources to ensure that the security of the school's ICT systems is maintained and to ensure that users comply fully with the terms of this policy. This should include suitable training to promote the proper use of ICT systems and to conform to the Policy.

The Headteacher must ensure that adequate procedures are established in respect of ICT security following changes in staff roles or when staff leave a post with the school.

## 15 Review of the Policy

This policy will be subject to regular review by the Local Governing Body of the school

# Password Protection Policy

## Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Thomas Adams resources. All users, including contractors and vendors with access to Thomas Adams systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at Thomas Adams, has access to the Thomas Adams network, or stores any non-public Thomas Adams information.

## Policy

1. Passwords for all systems should consist of 8 or more characters, consisting capital letters, lower case and numbers.
2. Where possible, users must use unique or a varied password between systems unless the system in question has synchronised single sign on.
3. User accounts that have high system-level privileges must have a unique password from all other accounts.
4. Users are automatically prompted by individual systems to change passwords on at least a quarterly basis.
5. Passwords must not be revealed over the phone to anyone.
6. Do not write down passwords and store them anywhere that isn’t secure.
7. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
8. Passwords must not be shared with anyone. All passwords are to be treated as sensitive.
9. Passwords must not be inserted into email messages or other messaging services.
10. Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers, family members while on vacation.
11. Do not leave any pc, laptop or device unlocked while unattended. Any unattended device must be locked or logged off.
12. Two factor authentication must be used where breaches of passwords have been made.

# Appendix A - IT Acceptable Use Policy and Resource Regulations

## 1 General

1.1 For the purposes of this policy the School network consists of all connected computer systems in the School, College and Boarding House.

1.2 Several students wish to connect their personal laptops to the School network. This can have great educational benefits, however, some regulation of access is necessary to balance loads on the system and to avoid misuse of the facilities. Students are granted access to School IT resources both workstations and the connected network only in terms of this policy and the condition that they observe these regulations.

1.3 There is no expectation of privacy on computers connected to the School systems. Both technical and teaching staff may examine a student's laptop for educational, technical or disciplinary reasons at any time.

1.4 Before a laptop is connected to the network, the user must ensure that it has appropriate virus checker, firewall software and an automatically updated version of the operating system to avoid the risk of damage to the School network. If unsure of how to complete this process – seek IT support from Technicians.

1.5 The School takes all reasonable steps to protect the network from harmful software and other threats, however, the school cannot accept responsibility for any damage which occurs to a student's computer or software as a result of connecting to the network or of transferring any data or information from the network

## 2 Availability and Use of Facilities

2.1 The computing facilities are made available on the understanding that they may only be used for purposes related to the user's programme of study or area of work and not for profit, entertainment or other unrelated purposes. Students playing games is expressly forbidden except under the direction of a member of the teaching staff.

2.2 Users must treat with respect any other computers, users and services accessed through the use of School facilities and are subject to the regulations imposed by the respective service providers.

2.3 No user shall modify a computer's software, settings or other stored information; or attempt to access, copy, modify or disseminate information which is not intended for their use or bypass any security systems that are in place for the users safety. If they are aware of methods of doing this they will not instruct others in such methods.

2.4 Users must not cause any unnecessary disturbance to other computer users.

2.5 The transmission, storage or collection of offensive, obscene or harassing material is strictly forbidden. If there is any doubt as to whether particular materials are acceptable then students should query this with the IT staff who will make a decision on it.

2.6 Users are responsible for monitoring and if necessary, rejecting any materials they have received/ accessed.

2.7 The unlicensed use or copying of software is regarded as theft. It is the user's responsibility to ensure that they do not violate any copyright laws by posting or distributing copyrighted material.

2.8 Plagiarism is unacceptable. Any material accessed on the computers should be used in an appropriate manner in assignments and its source suitably noted.

2.9 The School will cooperate with any external agency who believes a Thomas Adams user is in breach of these regulations.

2.10 All users to ensure their personal credentials are safe and secure at all times.

2.11 Users should also make sure that they have a strong password making use of numbers and letters.

## 3 Penalties

3.1 Users who fail to conform to this acceptable use policy may be required to pay for repairs to and replacement of any damaged equipment and the resources and time used by IT staff in investigating and correcting the situation.

3.2 Additionally students may have their access to IT facilities withdrawn by the IT staff. Serious cases or repeated offences may be reported to the Headteacher and may result in expulsion from the School.