The Thomas Adams School

Policy Statement

ICT E-mail and Internet Use Policy

Updated September 17 □

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 and Internet Use 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.

2 Responsibilities

2.1 Role of the Governors

To 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

2.2 Role of the Headteacher

To 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.

2.3 Role of the staff

To 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;

2.4 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.

3 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.

4 Resources

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

5 The Internet in the Curriculum

5.1 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.

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. A suitable alternative approach may be to have 2 entries on the site, one for school contacts and the other for personal/private use which is not available to school contacts.

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 Publishing

The school website 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 site 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, 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.

6 Internet Access

Authorised users are given a unique username and password generated by the Network Manager. Individual users are responsible for their own password security.

Filtering software is used to remove pages of unsuitable content according to a number of lists that contain the location of unsuitable content. These lists are updated frequently. 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

Pupils will be informed that their use of the internet will be monitored.

Access to inappropriate images and internet usage

There are no circumstances that will justify adults possessing indecent images of children. Staff 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 are 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, Shropshire Council should be informed and advice sought. The school should not attempt to investigate or evaluate the material themselves until such advice is received.

7 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.

8 Security

As noted above, the school and the LA have 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 screen, neither the school nor Shropshire Council can 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 LA are implemented where appropriate for the school
- Virus protection and firewall systems will be implemented and updated regularly
- 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

9 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 Network 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 work.

10 Review of the Policy

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

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 A number of 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 on 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 updating 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 student's programme of study and not for profit, entertainment or other unrelated purposes. The playing of 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 Students 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.