Woodham Academy
Policy Document

Student ICT User Policy

Summary

Woodham Academy is a forward-looking school dedicated to giving all young people the best possible start in an increasingly competitive and rapidly-changing world. We are determined that all of our students will develop a broad skill set, which includes reaching high standards in ICT and computing which is needed to progress into employment, further education or training.

We know that effective use of ICT can help to raise standards, enhance the quality of teaching and learning across the curriculum and enrich learning opportunities. As a highly innovative academy our staff are constantly developing and sharing good practice across the curriculum. ICT is increasingly used to support the professional work of staff, and enhance the management and administration of the school.

Alongside this determination to progress the use of new and existing technologies, is our recognition of the need for responsible and careful management of ICT access and resources.

Date adopted: 23rd June 2009

Review date: Annually

Last reviewed: September 2021

Key staff involved in the policy

Role	Name(s)
Head of ICT	Darren Smith

1.   Principles:

This policy is based upon the following principles:

- We are committed to promoting a technological culture
- The school has a duty to provide learning experiences that are needed for everyday life in the 21st century
- Used sensibly and responsibly, ICT is a valuable learning resource
- ICT can be used effectively to raise standards and enhance the quality of teaching and learning
- Access to ICT resources and services is an entitlement for all students who demonstrate a responsible approach

2.   Aims

This policy aims to give staff, students and their parents guidance on the safe and responsible use of school ICT resources including the internet. In addition, it outlines the measures that the school has implemented to ensure that staff and students can access the resources and facilities needed for learning.
Specifically, this policy will:

- Outline guidance for responsible use of hardware within school
- Give guidance to staff who borrow school devices
- Outline guidance for responsible use of the network
- Outline how the school will manage internet access for staff, students and other stakeholders
- Give guidance on the use of email

Guidance on the secure use of data through the Information Management System is documented in the data protection policy and summarised in the staff information guide.

3. Responsible use of hardware and ICT rooms

The ICT rooms and other computer facilities within the school are a resource to be shared by all members of the school. We all have a right to expect these facilities to be available to us, equally we have a responsibility to ensure that they are used correctly and remain available for all. The computer system (including email accounts) is owned by the school. It is a criminal offence to use a computer for a purpose not permitted by the system owner.

Use of ICT rooms and other facilities across school

The ICT rooms may be booked by any member of staff when not in timetabled use through a central booking system, Students should not be left unsupervised in ICT rooms under any circumstance.

Staff should:

- Ensure that all hardware is checked for damage or faults at the beginning of the lesson. Staff should report issues via the helpdesk.
- Check the ICT room for general tidiness – and report any incidences of litter or mess to the ICT support team.
- Remain observant and vigilant whilst using the ICT room. We must all take responsibility for ensuring that the rooms are kept tidy, litter free and damage free. Staff should also ensure that they are confident that students are engaged in approved activities throughout the lesson.
- Encourage students to be responsible ICT users, and to print only when essential and in black and white if possible.
- At the end of the lesson, ensure that the rooms are left tidy with chairs pushed under the tables, litter free, and that any damage or fault has been reported to the ICT team.
- Observe the "No food or drink" rule in the ICT rooms.

Students should:

- Check their workstation, and immediately report any damage or faults with hardware to the subject teacher.
- Observe the "No food or drink" rule in the ICT rooms.
- Only use the resources for the specified activities.
- Log out of any accounts, push chairs under and leave their workspace neat and tidy.

Please note that wilful or malicious damage to ICT equipment will result in disciplinary action, and may result in the student or their parents being charged with the costs of replacement or repair and/or referral to the police, subject to approval from the Headteacher or another member of Leadership Group.

Staff laptops / loan devices

Laptops, computers or other ICT devices on loan from the school remain the property of the school, and should only be used for approved activities. All devices must be password protected. They must be made available to the ICT support team for inspection or updating purposes as and when required. Staff must ensure that any laptop or other loan equipment is cared for responsibly, and if removed from the school site for use at home, then it must be covered by the member of staff's House Contents Insurance. Staff will be required to sign an equipment loan agreement which outlines the terms of use. Any damage or faults with hardware must be reported to the ICT support team immediately and the equipment surrendered for checking.

4. Responsible use of the network

Staff and students must:

- Never allow anybody else to use their account.
- Only ever logon to the network using their own account username and password.
- Always keep logon details private.
- Change their password IMMEDIATELY if they believe that someone else knows it.
- Never give login details to any other party.
- Never attempt to install any software or hardware on the school network.
- Never attempt to save any executable files or programs on the network
- Never download files from unknown sources.
- Never attempt to bypass any security measures including filters.
- Never attempt to upload any files that may contain viruses or malicious content
- Regularly check portable storage devices for viruses – please see point 8 Staff Code of Conduct.
- Monitor student usage of ICT resources during their lessons and take appropriate action when required.

Additional guidance relating to Data Protection, including information on how staff should deal with student data (for example when completing school reports) can be found in our Data Protection policy.

Other stakeholders (including parents, DCC staff & governors)

Where parents or other stakeholders have been given access to the network, they accept the same responsibilities as members of staff in terms of network security. All adults accessing the network must do so responsibly.

5.   Responsible use of the internet and electronic communication

Used correctly, the internet and electronic communication can enhance learning, provide enrichment opportunities and provide valuable resources.
The school ICT support team will ensure that all reasonable precautions are taken to ensure that users only access appropriate material. However, due to the nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed or consequences of internet access.

It is extremely important that staff and students are clear that in exercising the right to access the internet and electronic communication through the school network, they accept the responsibility to adhere to the following:

The internet:

- Sites and materials accessed must be appropriate to approved activities.
- If unsuitable websites are inadvertently discovered by staff or students, the web address and if appropriate the nature of the content MUST be reported to the ICT network manager IMMEDIATELY.
- Staff and students will not be allowed access to public or unregulated chat rooms.
- Staff and students must not deliberately attempt to bypass filters or security measures.

The ICT support team will ensure that all reasonable measures are regularly undertaken to identify, assess and minimise risks to staff and students through internet access.

Filters and email

All internet access and email communications may be filtered, recorded and archived, and as such may be reviewed or recalled if a breach of the school ICT user policy is suspected.

Electronic communications:

- Staff and students should remember that electronic communications should be written carefully and politely, as messages may be forwarded or printed and seen by unexpected readers.
- Staff and students are responsible for the electronic communications that they send. Emails sent using school email addresses will carry a disclaimer.
- Students should only use their email to correspond with people they know – or who have been approved by their teacher
- Students should NEVER give out home addresses, phone numbers and other personal details by email
- Staff and students should IMMEDIATELY report any messages that could cause offence, upset or distress Staff and students should NOT send email or other electronic communications from another person's account
- Staff and students should NOT use their school email account to sign up for newsletters, bulletins or other updates that are not directly related to the work of the school
- Staff should ensure that professional levels of language and content are used for emails and other electronic communications
- Staff should ensure that electronic communications are transparent, and not open to misinterpretation.

If there is just cause the ICT support team may monitor electronic communications and internet sites for unsuitable content. Any monitoring of staff accounts will be authorised by a senior member of staff. Staff may or may not be informed by leadership team if their account is monitored depending upon the nature of the monitoring request.

6.   Use of social networking sites

The use of social networking sites using the school network is prohibited for students. The school requires staff to take a responsible approach to their personal use of social networks, and to regularly review their use in light of their professional responsibilities. Passwords and security settings MUST be kept private. Further advice can be seen in the staff code of conduct policy and on various teaching union websites.
Students who are found to be using social networking sites to make derogatory comments about the school, other students or members of staff will be subject to disciplinary procedures.

7.   School website

The website will be regularly updated and maintained.

8.   Photography and video

Photography or filming of Woodham students will only take place under appropriate supervision. Photographs or video of activities involving Woodham Academy students may be used for displays, publications (such as the prospectus and parent mailings), our website and the local press. Where photography or filming is carried out by the media, individual students will only be named if there is a specific reason to do so (for example if they have won a prize), and home addresses or other contact details will never be given out. Images that might cause embarrassment or distress will not be used, nor will images be associated with material on issues that are sensitive. Woodham Academy will seek permission from parents on admission to the school for students to be included in school photographs. Consent will be reviewed each academic year. If parents do NOT want their children to be included in school photographs, then this should be indicated on the consent form and this wish will be respected. Parents have the right to withdraw consent at any time.
If parents wish to attend functions, extra-curricular activities, or other events and take photographs of their own son / daughter and other students, parents should remain sensitive to the rights of all students, only take appropriate images, and try not to disrupt or interrupt concerts, performances etc.
The ICT support team will regularly review images held by the school and delete unwanted and out of date material. All photographs and images taken on behalf of Woodham Academy remain the property of the school and are copyrighted unless specified otherwise. Staff will not store photographs or video of Woodham Academy students on their home computers and personal electronic devices.

9.   Safe disposal of ICT equipment

The ICT team will ensure that all disposal of ICT equipment is carried out in line with current government guidelines and in accordance with the Directive on Waste Electrical and Electronic Equipment (WEEE, 2007). All ICT equipment will be recycled where possible. All data will be removed from any ICT equipment prior to disposal in line with our Data Protection policy. Only the ICT support team should dispose of ICT equipment.

10.   Breaches of the policy

Breaches of the guidelines within this policy will be dealt with in accordance with our behaviour policy, anti-bullying policy or other relevant policies.
Students who misuse ICT or use ICT in an irresponsible way will be subject to appropriate and proportionate sanctions or measures as outlined in the school behaviour policy, anti-bullying policy, equality and diversity policies and child protection policy.
Staff who misuse ICT, their school account, or school resources will be reported to the Leadership Group and may be subject to disciplinary proceedings.
Staff or students who use ICT to undertake illegal activities may be reported to the police in addition to sanctions or measures imposed by the school.

11.   Monitoring and Review

Implementation of the policy will be monitored by IT Network Manager and Mr D Morgans. The policy will be reviewed regularly to respond to and take account of emerging technologies. Any failure of the policy should be reported immediately to Leadership Group and the Governors, who maintain overall responsibility for the implementation of the policy.

12.   Please refer to Social Media policy and IT & Communications Systems policy.