WEDNESFIELD HIGH
SPECIALIST ENGINEERING ACADEMY

ICT POLICY

Author	Revision Number	Date of Ratification at JNC	Review date
Mr Simon Whitehouse	2		October 2017

Policy adopted by the LAB of:		Date:	
Signed by the Chair of the LAB:		Print:	

Information Communication Technology (ICT) – Policy Statement

The aims of the ICT policy are to plan and implement strategies and construct and manage systems which support and further the education of students with regard to information technology and its use in the modern world.

Overall, this policy will:

- establish a framework for publicising, implementing and monitoring the acceptable use of ICT systems;
- identify procedures for the assessment of students with regard to their ICT knowledge and skills;
- indicate ways in which ICT targets are being integrated across all areas of the academy's work;
- ensure the effective monitoring and evaluation of ICT systems;
- promote an academy-wide culture of ICT development;
- encourage the effective and efficient deployment of all ICT resources;

Acceptable Use

The ICT Coordinator will be the designated E-Safety Officer

A priority for ICT development across the academy will be to ensure that all users will engage with ICT systems in a safe and acceptable manner.

Teaching and Learning

The academy will ensure the development and implementation of an appropriate ICT curriculum which meets the needs of all learners.

The academy will identify and focus on the user's skills and highlight areas for action to develop ICT knowledge and application amongst all stakeholders.

ICT will be used to inform and enhance the lesson planning process.

ICT will be used to promote communication between all stakeholders.

Monitoring, Evaluation and Review

The ICT Strategy Group on behalf of the Local Advisory Board (LAB) and the Headteacher will ensure that the policy is implemented. The policy will be reviewed at least annually.

The Headteacher and LAB members will receive regular reports about policy implementation and the inherent monitoring of ICT management systems.

The monitoring of ICT systems will involve regular and whole-academy evaluation of all matters relating to e-safety.

ICT – Policy In to Practice

The academy believes that ICT is an integral part of the 21st century curriculum. Students must leave the academy with knowledge of ICT and its applications such that they will not be disadvantaged as they attempt to make their way in an increasingly digital world.

ICT will be delivered across subjects as an integrated programme of knowledge and skills development. The progress of students will be monitored by the ICT Co-ordinator. He/she will arrange for the necessary systems to be in place whereby levels of ability are assessed and appropriate ICT experiences developed in consultation with subject teachers. Where appropriate, qualified ICT staff will work in and across departments to enhance opportunities for students to see the advantages of ICT application and non-specialist ICT staff may benefit from seeing the use of technology as an aid to learning.

The academy will use a fully-supported Learning Platform as a vehicle for delivering ICT programmes. The Platform will also facilitate communication between various members of the academy community, including parents/carers. All members of the academy community will be encouraged to engage with the Platform as generators and/or recipients of information.

All members of the academy will be asked to contribute to regular feedback about the opportunities for using ICT to support teaching and learning and enhance communication. The academy will collate all responses and show that views of stakeholders are being considered and, where appropriate, acted upon.

Deliverers of learning programmes will be given opportunities to work collaboratively so as to develop a wide range of resources to support the learning of students with differing experiences and levels of ability. Teachers will be able to work confidently using a range of digital devices in a range of learning contexts.

All members of the academy community will be given opportunities to enhance their knowledge of ICT and its applications. Training will be made available to suit personal needs. CPD will be scheduled at convenient times – using the Platform as appropriate to provide an online learning community for remote access.

The ICT Co-ordinator will work with Technicians to ensure the ICT systems are robust and fit for purpose. This includes software as well as hardware. Departments will share responsibilities, as assigned by the Co-ordinator, for monitoring the use and status of software and appropriate licences. There may also be a shared responsibility for peripherals where these are assigned to departments or to administration areas.

A Strategic Management Group will be responsible for the monitoring of this policy and practice in the first instance. This group will formulate strategies to ensure that the objectives with regard to ICT are assessed and reviewed. This group will report regularly to Senior Leaders and to LAB members about the success of ICT as measured by exam results, feedback from users, levels of misuse, the range of devices employed in learning experiences and the CPD record of practitioners across the academy.

ICT Acceptable Use – Policy In to Practice

Guidelines for Staff

The academy has provided computers for use by staff as an important tool for teaching, learning, and administration of the academy. Use of academy computers, by both members of staff and students, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to Mr G Kalair (Head of ICT) in the first instance.

All members of staff have a responsibility to use the academy's computer system in a professional, lawful and ethical manner. Deliberate abuse of the academy's computer system may result in disciplinary action.

Please note that use of the academy network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the academy and staff, to safeguard the reputation of the academy, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the academy recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the academy neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the academy.

Computer Security and Data Protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. If you do so, you will be required to change your password immediately.
- You **must not allow a student to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you **must** ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or ICT device) unless that storage system is encrypted and approved for such use by the academy.
- You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the academy.
- When publishing or transmitting non-sensitive material outside of the academy, steps **must** be taken to protect the identity of any student whose parents have requested this.
- If you use an ICT device at home for work purposes, you **must** ensure that any academy-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You **must** make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the academy) or an ICT device.

- You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken offsite is not routinely insured by the academy. If you take any academy computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.

Personal Use

The academy recognises that occasional personal use of the academy's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- **must** comply with all other conditions of this Acceptable Use Policy (AUP) as they apply to non-personal use, and all other academy policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by the academy.

Personal use is permitted at the discretion of the academy and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated ICT device or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by academy's normal rules on electrical safety testing.
- You must not connect ICT device equipment to academy computer equipment without prior approval from IT Network staff, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation on harmful software onto the academy computer system.

Conduct

- You must at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference or gender-related slurs or jokes;
- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system;
- You must not intentionally damage, disable, or otherwise harm the operation of computers.

- You must make efforts not to intentionally waste resources. Examples of resource wastage include:

  - Excessive downloading of material from the internet;
  - Excessive storage of unnecessary files on the network storage areas;
  - Use of computer printers to produce class sets of materials, instead of using photocopiers.

- You should avoid eating or drinking around computer equipment.
- All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP) in addition to the guidelines here.

Use of Social Networking Websites and Online Forums

Staff must take care when using social networking websites such as Facebook or Twitter, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any student to access personal information you post on a social networking site. In particular:

- Please **do not** add a student to your 'friends list';
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility;
- You should avoid contacting any student privately via a social networking website, even for academy-related purposes;
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the academy – even if their online activities are entirely unrelated to the academy:

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the academy.
- You should not post any material online which can be clearly linked to the academy and which may damage the academy's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a student, that could potentially be used to embarrass, harass, or defame the subject.
- The academy will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, Instant Message (IM) and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or academy.

- Teachers' official blogs or wikis should be password protected and run from the academy website. Teachers are advised not to run social network spaces for student use on a personal basis.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.
- Students will be advised not to publish specific and detailed private thoughts.
- Students will be made aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Use of E-mail

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the academy. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the academy via e-mail without proper authorisation.
- All academy e-mail you send should have a signature containing your name, job title and the name of the academy.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the academy.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The academy will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Student Use

Students must be supervised at all times when using academy computer equipment. When arranging use of computer facilities for students, you must ensure supervision is available.
Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for students is enforced. Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by students.

Privacy

Use of the academy computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the academy to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session.

In particular, the academy does keep a complete record of sites visited on the Internet by both students and staff; however, usernames and passwords used on those sites are NOT monitored or recorded.

You should avoid storing sensitive personal information on the academy computer system that is unrelated to academy activities (such as personal passwords, photographs, or financial information). The academy may also use measures to audit use of computer systems for performance and diagnostic purposes.

Use of the academy computer system indicates your consent to the above described monitoring taking place.

Confidentiality and Copyright

Respect the work and ownership rights of people outside the academy, as well as other staff or students. You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the academy computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

You **must** consult a member of IT Network staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the academy is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the academy's systems.

As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the academy or capable of being used or adapted for use within the academy shall be immediately disclosed to the academy and shall to the extent permitted by law belong to and be the absolute property of the academy.

Reporting Problems with the Computer System

It is the job of the IT Network Manager to ensure that the academy computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem **must** be reported via the online Support Request system.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Network staff **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable.

Reporting Breaches of this Policy

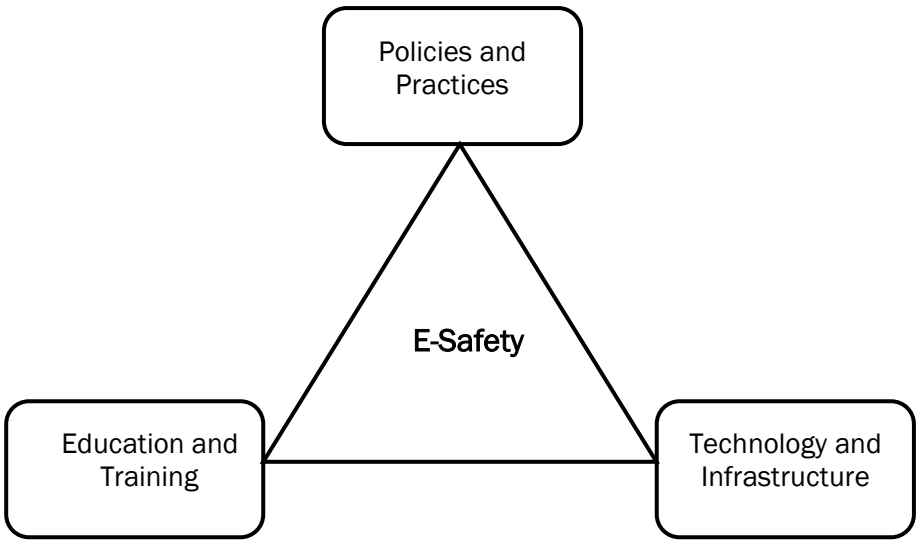
All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform a member of the IT Network staff, or the Headteacher, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within academy that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a student via the academy computer system.
- any damage of equipment of both portable and fixed IT hardware.

Reports should be made either via email or the online Support Request system. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.



Acceptable Use – Additional Information and Guidance

Developing safe academy web sites

The academy website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the academy's website for information. The academy will have a designated member of staff who will oversee the construction and management of the website. Colleagues are invited to take an active part in the maintenance of contemporary website information. Before any contributions can go 'live' they will be approved by the website manager. No information or images (moving or still) of any individual student will be published without the prior and written permission of the student and his/her parent/carer. The following rules must apply:

- If the student is named, avoid using their photograph/video footage.
- If the photograph/video is used, avoid naming the student.

If the academy website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

Only use images of students in suitable dress to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at an academy play or sports day. However, photographs taken for official academy use, which are stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, students and students will be advised why they are being taken.

Links to any external websites will be thoroughly checked before inclusion on the academy website to ensure that the content is appropriate both to the academy and for the intended audience.

Text written by students will be reviewed before being published on the website. The academy will make sure that the work does not include the full name of the student, or reveal other personal information, such as membership of after academy clubs or any other details that could potentially identify them. The academy will make every effort to ensure that any contributions on the website will not offend or defame. Every effort will also be made to ensure that the academy does not infringe copyright or intellectual property rights through any content published on the website.

Use of Mobile Technology

Digital images - photographs and video clips - can now readily be taken using, e.g. mobile phones. The academy takes its responsibility towards ensuring the privacy of staff, students and visitors very seriously. Inappropriate use of mobile technology will not be tolerated. Any member of the academy community deemed to be in breach of this acceptable use policy may face exclusion from the academy and/or referral of the incident to other authorities, e.g. The Police. Staff are advised not to use their personal phone or camera for recording student activities, e.g. field trip. If personal equipment is being used it should be registered with the academy and a clear undertaking made that photographs will be transferred to the academy network and will not be stored at home or on memory sticks and used for any other purpose than academy approved business.

Technical

Digital images/video of students will be stored securely on the academy network and old images deleted after a reasonable period, or when the student has left the academy. When saving pictures, the image file will be appropriately named. Students' names will not be used in image file names or in <ALT> tag references when published on the web.

[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]

Additional Information/Clarification

Please contact any member of SLT.