Digital Technology and Acceptable Usage Policy

Reviewed: October 2016

This document applies to all academies and operations of the Vale Academy Trust.

Document Control			
Review period	24 Months	Next review	October 2018
Owner	Head of IT	Approver	Board of Directors
Category	Public	Type	Global

Definition

Digital Technology (DT) has the potential to improve the quality of teaching and learning across the Curriculum. Technological innovation means there is an increasing need for a greater level of technological knowledge and awareness amongst the population as a whole. The effective use of DT will help to produce a population which feels comfortable with the new technology, is able to access life-long learning opportunities through the use of DT and can adapt to the rapid changes in this field.

Aims

Across the Vale Academy Trust we aim to:

- ensure all staff and young people are confident, competent and independent users of digital resources
- ensure all staff and young people are trained in e-Safety protocols with links to Behaviour and Safeguarding policies
- develop young people's ability to use digital technology appropriately and choose software suitable for a particular task
- develop an appreciation of the use of digital technology in the context of the wider world
- enrich learning and develop digital technology skills through curriculum context linked to Computer Science
- use digital technology in a range of situations e.g. problem solving, computational thinking, independent learning skills and group activities
- promote an environment of care and respect for the equipment

Roles & Responsibilities

Headteachers are responsible for ensuring the procedures are in place to implement this policy.
The VAT Project Lead is responsible for providing the technology and support to enable the procedures.

Digital Resources

Internet

Young people and staff can be granted internet access via the Academy network and where available the Wi-Fi network. In order to access the internet a user must log on with their username and password, which is allocated by the digital technology team. Users have to indicate they accept and understand the Acceptable Usage Policy (AUP) before access is granted. User passwords need to be secure and changed on a regular basis.

Young people need to be taught the risks involved with being on-line and steps they can take to ensure e-Safety.

The Headteacher is responsible for:

- Appropriately worded AUP
- Ensuring young people are taught to be critically aware of the materials they access before they accept its accuracy
- Young people are taught what content is acceptable and what is unacceptable and are encouraged to report immediately any offensive materials which they may access
- Young people and staff passwords are secure and changed on a regular basis

The VAT Project Lead is responsible for:

- Ensuring the “Prevent” Strategy is included within website monitoring
- Ensure the set-up of filtering safeguards for each school
- Provide support to ensure each school creates and adopt their own age appropriate “Acceptable User Policy”
- Provide password strength and frequency of update guidelines

Multimedia websites

There is a growing industry of companies providing video, homework, revision, and reference websites from YouTube through to the BBC. Reference material must be reviewed to ensure they are relevant and age appropriate. Sites that involve sharing of personal data such as young people’s email addresses must be approved with the school privacy notice updated.

Staff must never post videos or images of students on to external websites without approval from within the school and written permission from parents.

The Headteacher is responsible for:

- Ensuring staff review reference material
- Do not share young people’s personal data and images without school and parent consent

Social Networking websites
Members of staff must not initiate contact with, or respond to contact from, current students through social networking sites from personal accounts. In particular, staff must ensure that the privacy settings on social networking accounts do not allow students to access personal information about them, including the ability to download photographs. Staff must not post derogatory comments against other colleagues, their employer or young people within the school.

Members of staff wishing to set up Facebook (or similar) groups for educational reasons must approach the VAT Project Lead in writing for advice.

The Headteacher is responsible for:

- Ensuring staff are trained and understand the implications of inappropriately using social media.

The VAT Project Lead is responsible for:

- Provide advice when setting up social media site e.g. Facebook, twitter etc.

VLE (King Alfred's school and all governors)
King Alfred's hosts its own Virtual Learning Environment (VLE). The VLE is based on Microsoft SharePoint software and allows young people, parents, governors and staff access to a wide range of educational resources, sensitive documents and general information. Users are able to access the VLE at any time and from anywhere by using their network logon details. Users using external computers are responsible for ensuring that they log-off the VLE to prevent access to the system by those unauthorised to do so. The VLE is backed-up and should be deployed for storing student work and sensitive student data.

The Headteacher is responsible for:

- Ensuring that lesson resources and sensitive student data are appropriately stored.

The VAT Project Lead is responsible for:

- Providing staff training for Class sites which should be used to hold lesson information and student work. Sensitive student information should be stored in the department folders.
- Ensuring data can be recovered in the event of a disaster or loss of work.

Email
The academy email is part of the free Office365 service offered by Microsoft. E-mail communication should not be considered private or secure and therefore staff must consider carefully the content of potentially sensitive emails. When writing an email bear in mind that 'Freedom of Information' requests for copies of emails may be made by individuals with a justifiable reason.

Staff must not use their personal e-mail addresses for college business to protect their privacy. Members of staff may use their college e-mail addresses for appropriate personal use.

Emails between staff, governors, parents and students should be professional and focused on college work. Inappropriate emails will be dealt with in accordance to the college Child Protection (safeguarding and promoting the welfare of pupils) and staff Disciplinary, Conduct and Grievance policies.

As part of the Office365 package staff and young people and make use of OneDrive to securely store data in the cloud.

We retain emails for 365 days after user deletion.

The Headteacher is responsible for:
- Ensuring that staff use emails appropriately for both internal and external communications.
- Ensuring staff share data appropriately (see Data Storage and Sharing).

The VAT Project Lead is responsible for:
- Providing staff training for the Office365 package.

Personal electronic equipment
Both staff and students may bring personal electronic equipment, e.g. netbooks, laptops, tablets, and digital cameras into college to use for educational purposes.

The following applies:
- Staff personal computers should not be connected by cables to academy equipment
- Personal computers must have up to date antivirus / security software
- Student data must not be saved to staff personal devices
- Personal cameras must use a memory card supplied by the school
- Personal equipment must not be charged unless they have passed a Portable Appliance Test (PAT test).

The Headteacher is responsible for:
- Ensuring that staff understand and adhere to the policy

The VAT Project Lead is responsible for:
- Ensuring appropriate software is introduced to meet the policy.

Data Storage and Sharing
Staff need to be aware that under the Data Protection Act security needs to be in place to prevent unauthorised access. In addition data must not be stored outside the EU, Staff therefore need to ensure the following:

- Student data is stored using recognised Academy storage mediums
- Unencrypted memory sticks must not be used
- Personal accounts to cloud services must not be used

The Headteacher is responsible for:

- Ensuring that staff understand and adhere to the policy

The VAT Project Lead is responsible for:

- Ensuring appropriate software and encrypted memory sticks are introduced to meet the policy.

E-Safety
The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will included in programmes of work and embedded in PSHE and SRE.

Safeguarding
All teachers are responsible for monitoring and responding to issues of e-safety and cyber bullying. As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups through Safeguarding training.

Parents will be made aware of any issues arising and any sanctions which may be imposed.

Students are taught about issues relating to e-safety and cyber bullying through lessons, assemblies, and PSHE activities and understand that sanctions may be imposed if they use the facilities in an inappropriate manner. Students are taught to report immediately any offensive messages or if they feel uncomfortable with any messages that they receive.

Monitoring software should be in place to alert Safeguarding staff of incidents caused by inappropriate IT usage.

Acceptable Usage
Each school is responsible for creating an appropriate age related Acceptable Usage Policy in conjunction with the VAT Project Lead.

Health and Safety
All young people must receive introductory sessions dealing with Health and Safety issues that can arise from using IT equipment. Staff using digital technology must ensure Health and Safety guidelines are not breached.

All equipment is checked annually under the Electricity at Work Regulation 1989. A detailed inventory is kept up to date by the central IT Team who ensure all equipment is checked. New equipment is added to the inventory on arrival.

Security
Staff must not leave laptops or any other portable equipment unattended in classrooms, cars or any other place where the equipment could be stolen. Staff must ensure the use of an appropriately secure password for all academy systems. A secure password includes a combination of uppercase letters, lowercase letters, symbols and numbers.

Passwords must be changed on periodic basis and no password can be re-used.

The Headteacher is responsible for:

- Ensuring that staff are trained to recognise the following:
    - Safe online
    - Acceptable Usage Policy
    - Radicalisation
    - Cyber Bullying
    - Secure passwords
    - Health and Safety guidelines when using IT equipment

The VAT Project Lead is responsible for:

- Providing support
- http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals