Diverse Academies
Learning Partnership

Acceptable use of Computers and Internet
May 2018

Office use

Published: May 2018	**Next review:** May 2019	**Statutory/non:** NON	**Lead:** Pete Richardson DALP
Associated documents:			
Information Security Policy Managing User Access Policy Anti Virus Policy Physical Security Policy		Patch Management Policy BYOD Policy IT Investigations and Data Access Policy IS Incident Management Policy	
Links to:			
Data Protection Act 1998 DALP Communications Policy/guidelines			

Contents

1 Policy Statement and Introduction

1.1 Diverse Academy Learning Partnership (DALP) provides 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 this policy. Please ensure you understand your responsibilities under this policy and direct any questions or concerns to the IT Service Manager of your academy 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 (including possible termination), and civil and/or criminal liability.

1.2 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.

1.3 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

2 Scope and Purpose of the Policy

2.1 This policy applies to all employees, governors, volunteers, visitors and any contractors using our ICT facilities. Ensuring ICT is used correctly and properly and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy, you should speak to the IT Service Manager at your academy or a member of the Leadership Team.

2.2 The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect DALP and its employees from risk.

2.3 Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. A serious breach of this policy may be considered as gross misconduct which could lead to dismissal. If we are required to investigate a breach of this policy, you will be required to share relevant password and login details.

2.5 If you reasonably believe that a colleague has breached this policy you should report it without delay to your line manager or a senior member of staff.

3 Roles and Responsibilities

3.1 The Diverse Academy Learning Partnership (DALP) has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. The Trusts have delegated day-to-day responsibility for operating the policy and ensuring its maintenance and review to the IT service management of each academy.

4 Computer Security and Data Protection

4.1 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 if you do so, you will be required to change your password immediately.

4.2 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.

4.3 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.

4.4 The use of USB memory sticks and portable hard drives are strongly discouraged unless for exam or presentation use. More secure methods for transporting data are available via Microsoft OneDrive or Academy VPN/Remote access functions. USB storage devices pose unnecessary risks around data breaches and IT Security.

4.5 Do not use non IT-authorised third party hosting services, like Dropbox or Google Mail, when processing data

4.6 When publishing or transmitting non-sensitive material outside of the academy, you must take steps to protect the identity of any student whose parents have requested this.

4.7 If you use a personal computer 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.

4.8 You must make your own backup of data kept on any storage system other than the network storage drives or your ‘My Documents’ folder.

4.9 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.

4.10 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 theft, loss or damage.

4.12 In the event of theft, loss or damage you must contact IT Support immediately.

5 Personal Use

5.1 DALP recognises that occasional personal use of the organisation'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

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

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

6 Conduct

6.1 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

6.2 You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.

6.3 You must not intentionally damage, disable, or otherwise harm the operation of computers.

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

a) Excessive downloading of material from the Internet;
b) Excessive storage of unnecessary files on the network storage areas
c) Excessive use of local printers to produce class sets of materials, instead of using photocopiers

6.5 You should avoid eating or drinking around computer equipment.

6.6 All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP)

7 Use of Social Networking websites and online forums

7.1 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:

a) You must not add a student to your 'friends list'.
b) We strongly advise that your personal information is not accessible via a 'Public' setting, but recommend it is set to a 'Friends only' level of visibility.
c) You should avoid contacting any student privately via a social networking website, even for academy-related purposes.
d) 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.
e) 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 DALP – even if their online activities are entirely unrelated to DALP.
f) Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for DALP.
g) You should not post any material online that can be clearly linked to DALP that may damage the DALP's reputation or bring the organisation into disrepute.
h) 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.

8 Use of Email

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

a) 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.
b) 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 organisation via e-mail without proper authorisation.
c) All DALP/ academy e-mails will be identical, a professional footer containing: name, job title, name of the academy, office telephone number, extension number, work mobile number, email address, twitter details.
d) All e-mail accounts must have an 'out of office' professional message when the account holder is absent ie on leave etc.

e) 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 DALP.
f) Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. DALP 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.
g) You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

9 Supervision of Student Use

9.1 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.

9.2 Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for students is enforced.

9.3 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.

10 Mobile Phone communication

a) Staff whom access DALP/academy emails via their mobile phone must ensure the device has passcode or suitable security in the event the device becomes lost or stolen
b) Staff must not give their home telephone number or their personal mobile phone number to students.
c) Photographs and videos of students must not be taken with personal mobile phones/devices
d) Staff are advised not to make use of students' mobile phone numbers either to make or receive phone calls or to send to or receive from student's text messages other than for approved DALP/academy business.
e) Staff should only communicate electronically with students from academy accounts on approved academy business, e.g. coursework.
f) Staff should not enter into instant messaging communications with students.

11 Confidentiality and Copyright

a) Respect the work and ownership rights of people outside DALP/academy, as well as other staff or students.
b) 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.

c) You must consult a member of IT Support 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 DALP/academy's systems.

d) 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 DALP/academy or capable of being used or adapted for use within DALP/academy shall be immediately disclosed to DALP/academy and shall to the extent permitted by law belong to and be the absolute property of DALP.

e) By storing or creating any personal documents or files on the DALP/academy computer system, you grant DALP/the academy a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way DALP/ the academy sees fit.

12 Reporting Problems with the Computer System

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

a) 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 or Email

b) If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Support staff immediately.

c) 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

13 Reporting Breaches of this Policy

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

a) any websites accessible from within a DALP academy that you feel are unsuitable for staff or student consumption;

b) any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;

c) any breaches, or attempted breaches, of computer security; or

d) any instance of bullying or harassment suffered by you, another member of staff, or a student via the academy computer system.

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

14 Review and Evaluation

14.1 This policy is reviewed annually by the Trusts we will monitor the application and outcomes of this policy to ensure it is working effectively. This policy will be reviewed 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.

14.2 "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and student SEND data. This list is not exhaustive. Further information can be found in the academy's Data Protection Policy.