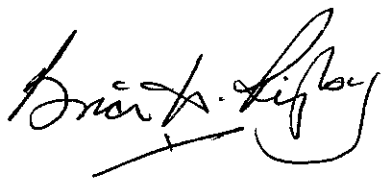
THE DEAN TRUST
Believe Achieve Succeed

ACCEPTABLE USAGE POLICY (COMPUTERS, INTERNET, EMAIL & MOBILE DEVICES)

STUDENTS

Version	Review Date	Author Notes
1.3	February 2016	Group Policy – to be reviewed by Dean Trust Board March 2016; Author: Mike Ward

Policy Reviewed	February 2016
Next Review:	February 2017
Signature of Chair of Trustees:	

Contents

VERSION	Date	Change Author	Description
1.0	1st July, 2010	Rashid Mogradia	Draft Version
1.1	17th July, 2013	Richard Middlebrook	Omitted "students" will only use the computers for School work" – implied in the Policy
1.2	3rd February 2016	Mike Ward	Complete policy re-write, new "base version" of policy created
1.3	4th February 2016	Ruth Warburton	Reformatted to reflect DT wide policy Removal of Vicky Beer as signatory Addition of clause: Students will ensure that all electronic communications with students and staff maintain a respectful and civil tone.

Sign off:

NAME	POSITION	SIGNATURE	DATE
Mr T Kapur	Chief Executive and Academy Principal		
Mr L McConaghie	Head of School (Broadoak School)		
Mr P Heath	Head of School (Forest Gate Academy)		
Mr A Moloney	Head of School (Ashton on Mersey)		
Mr B Bridden	Head Teacher (Lord Derby Academy)		
Ms S Finlay	Head of School (Dean Trust Ardwick)		
Mrs Ruth Harrison	Head of School (Park View Academy)		
Mr N David	Chief Finance Officer		
Mr M Ward	Group IT Manager		

THE DEAN TRUST
Believe Achieve Succeed

IT Acceptable Usage Policy

(Student use)

February 2016

Executive Summary

This is an Acceptable Usage Policy for students of The Dean Trust (studying at one of its Schools). It describes the way in which IT systems can and cannot be used within local School networks and the wider Trust organisation. This policy includes the use of hardware devices, software, services and applications either owned or provided by the School / Trust, the individual or third parties for the use of students either on or off premises.

In addition, this guide also covers the use of Email, Mobile Devices and the Internet in order to safeguard the interest of the users, students, staff, governors and The Trust from computer misuse and access to inappropriate content whilst complying with the requirements of regulatory Acts and Laws.

This policy meets the requirements of the Companies Act 1985, the Computer Misuse Act 1990, the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Electronic Communications Act 2000.

As technology changes are frequent and often emerge much faster than robust policies can be created and associated risks identified, this policy is subject to continual changes and revisions in order to keep both employees, students and the employer protected in the safe use of technology.

Misuse or abuse of any computer system by students is a serious matter and may be dealt with under the local School's disciplinary procedures, students are reminded that if they are in any doubt as to what they are or are not allowed to do whilst using the School's computer systems, they should ask a member of staff or the IT Support Department who will be able to advise them of best practice.

Computers, Internet & Email

1. Students will only access the system using their own login and password, which they will keep secret and are prompted to change at least once a term.

2. Students will not allow others access to systems using their credentials.

3. Students will not access files belonging to anyone other than themselves.

4. Students will not engage in any activity that may threaten the integrity of the School's ICT Systems, or engage in any activity that attacks or corrupts internal or external systems.

5. Students will not bring in CD/DVD's/USB's or 'removable media' from outside of the School and use it on any of the School's Computer Systems – unless authorisation is given by a member of staff.

6. Students will not download / upload / copy any material onto the School network, which is not related to School work. Examples of files which should not be stored on the School network include (but are not limited to); computer programming scripts, viruses, MP3/MP4 files, videos files and copyrighted material, unless authorised to do so as part of their classes.

7. Students will not use the School Internet for personal financial gain, gambling, advertising, inciting hatred or political purposes.

8. Students will not post anonymous messages or forward SPAM emails.

9. Students will respect and ensure they do not breach the copyright of material found on the internet.

10. Students will not use the School network to access inappropriate material such as pornographic, racial or other offensive sites.

11. Students will not use Internet access on School systems to access chat rooms nor will they edit photographs or images of students and staff and post them onto Internet / social networking sites.

12. Students will report any unpleasant material or messages sent to them to a member of staff. These reports will be confidential and will help protect others.

13. The School maintains the right to check computer files and emails and may monitor the Internet sites visited.

14. Students will not give personal details, home addresses, telephone numbers or arrange to meet anyone via the Internet, unless a parent, carer or teacher has given them permission.

15. Students who cause wilful damage to the School's property, including ICT equipment will be charged for the repair / replacement of any damage.

16. Failure to comply with this policy may lead to a formal warning and a phone call home, which may in turn lead to a student being excluded from School.

17. If students have any concerns on information they find on the Internet, either relating to a fellow student or not, they must immediately inform a member of staff.

18. Breaching this AUP will result in parents / carers being informed and where necessary disciplinary action being taken.

19. Students will ensure that all electronic communications with students and staff maintain a respectful and civil tone.

Monitoring

The School accepts that the use of the Internet, Email & IT facilities are an extremely valuable legitimate business, school and research tool. However misuse of such a facility can have a detrimental effect on other users and potentially the School's public profile. As a result, the School monitors;

- The volume of Internet, network and email traffic, as a group and individually at the request of senior management or for the purposes of IT proactive fault resolution / strategy.
- The domain names and / or IP addresses of Internet sites visited and domain and / or IP addresses of email received.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use and monitoring is authorised by Senior Management or a member of the Executive Team.
- Data storage usage by individuals (this may include the volume of data, file types and legality of data).

Note: *The Dean Trust is committed to ensuring that any monitoring is undertaken with reference to the privacy of the user; and with regard to the Companies Act 1985, Computer Misuse Act 1990, the Data Protection Act 1998, the Human Rights Act 1998, the Freedom of Information Act 2000, the Electronic Communications Act 2000, the Regulation of Investigatory Powers Act 2000, and other Lawful Business Regulations now in force or enacted at a later date.*

Biometrics

The School uses a Biometrics finger print enrolment system as proof of identity when purchasing food and drink from any of its canteens / dining halls. In order to purchase food / drink from these areas, it is necessary for the School IT department to store finger print records and associate them with individuals.

These records are stored securely within the School's IT Servers and protected from non-authorised access or use. Information stored relating to individual users will only be provided to Police, upon official request and not used for any other purpose other than its primary usage (i.e. Biometrics Food Ordering)

Social Media

Social Media is becoming more integrated with both our personal and business lives, allowing us to digitally 'connect' with our friends, business clients, colleagues and more.

Users of Social Media must ensure the following policy points are followed at all times in relation to Social Media use either on the premises, off premises, or at any other time.

- Students must not 'connect with' 'follow' or 'friend' any members of staff on any Social Media accounts.
- Students must not send Private Messages (PM) to staff either past or present.
- Students are advised not to link any of their profile information to the Trust or School, for example "education" should not refer to Ashton on Mersey, Lord Derby Academy, Broadoak School, Forest Gate Academy or any other Trust Schools.
- Students should not refer to any member of staff, fellow students or the School in a derogatory or slanderous manner in the public realm (an example of this would be posting a status update about an individual in an adverse light).
- Schools within The Dean Trust have a duty of care for students and any form of bullying will not be tolerated within its schools, either on or off the premises. If students are being bullied, victimised or threatened through Social Media, they should inform a member of staff immediately and appropriate action will be taken.
- Students will ensure that all electronic communications with students and staff maintain a respectful and civil tone.

Malicious Damage

All students have a duty of care to look after technology devices used either solely by them or resources available and used throughout the rest of the school (e.g. laptops from secure trolleys) or fixed based machines based in classrooms / libraries.

The Trust accepts, that on occasion, damage can occur through accidental incidents and that this is a normal event in the daily use of devices such as laptops, tablets and fixed based machines.

In the event that an item of IT hardware is maliciously damaged, through either vandalism or otherwise, any resulting damage and associated repair costs will be invoiced to the parent / carer of the child in question.

THE DEAN TRUST
Believe Achieve Succeed

IT Acceptable Use Policy User Agreement

In order to use items of School hardware, software, services and peripherals, users need to agree to the IT Acceptable Usage Policy, herewith.

Please read the following statement carefully and if you are in agreement with this policy, please sign and date the agreement and provide a hard copy to the Group IT Manager. Upon completion, IT will complete all remaining fields and issue you with your device.

I ..... (insert name here), have read and fully understood all elements of the enclosed IT Acceptable Usage Policy and hereby agree to all rules and requirements mentioned within.

Student Signature: .....

Print: .....

Date: .....

As the Parent/Carer I grant permission for my son/daughter to use the school computers, email and internet. I understand that students will be held accountable for their own actions. I also understand that some material on the internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media

Parent / Carer Signature: .....

Print: .....

School.....