Djanogly Learning Trust

Acceptable Use of IT Policy

Department:	ICT
Author:	Head of Finance & ICT
Consultation Date:	July 2015
Date of issue:	July 2015
Date revised:	
Review date:	July 2018

DJANOGLY LEARNING TRUST

Acceptable Use of IT Policy

The Djanogly Learning Trust

The Djanogly Learning Trust (the Trust) is a multi-academy trust established in August 2011.

Under its governing articles of association the powers to run the Trust are held by the Board of Directors, which is supported by a Strategic Executive Team comprising the senior leaders from the Academies and the Trust.

Individual Academies within the Trust have delegated authority from the Board of Directors to their own Local Governing Bodies, which in turn are supported by their Head teacher or Principal.

This policy relates to all Trust Academies. Some procedures may vary across the Academies depending on context and stage of development.

1.0   Introduction

This policy is to provide clear guidance to all users of IT and equipment, staff, students and visitors across the Trust as to what is acceptable to do on the Internet and with IT equipment, and what is not. IT is an invaluable tool and this policy is designed to offer guidance to keep all users safe. If you feel that there is anything missing from this policy please feed back to the IT helpdesk who will look to add to future versions so we can all learn lessons from our IT experience and usefully share it with others.

2.0   Monitoring

All internet activity is logged by the Trust. These logs may be monitored by authorised Trust staff.

3.0   e-Mail

The use of e-mail is a critical means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff-based or pupil-based, within school or internationally. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

3.1 Managing e-Mail

● The Trust gives all staff their own e-mail account to use for all Trust business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and to avoid the risk of personal profile information being revealed

● It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The Trust e-mail account should be the account that is used for all school business

● Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

● A standard disclaimer is attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the Trust''.

● All e-mails should be written and checked carefully before sending, in the same way as a letter written on academy headed paper

● Staff sending e-mails to external organisations, parents or pupils are advised to cc. their Head teacher or line manager

● Pupils may only use academy approved accounts on the academy system and only under direct teacher supervision for educational purposes

● E-mails created or received as part of your job within the Trust will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You should therefore actively manage your e-mail account as follows:
  – Delete all e-mails of short-term value
  – Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

● All pupil e-mail users are expected to adhere to the generally accepted rules of good internet etiquette particularly in relation to the use of appropriate language; not revealing any personal details about themselves or others in e-mail communication; only arranging to meet anyone with specific permission and always virus checking attachments

● Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

● Staff must inform their line manager if they receive an offensive e-mail

- Pupils should be introduced to e-mail as part of the ICT Scheme of Work

- However you access your academy e-mail (whether directly, through webmail when away from the academy or on non-academy hardware) all the Trust's e-mail policies apply

3.2 Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please be aware of data protection principles. [Click here for the Data Protection Policy](#)

- Use your own Trust e-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path (link) to the file on the shared drive rather than sending attachments

- The Trust e-mail system is not to be used for personal advertising

3.3 Receiving e-Mails

- Check your e-mail account regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; Consult your network manager first

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of e-mails is not allowed

4.0 Passwords

- Passwords must contain a minimum of six characters and be difficult to guess. However, where possible they should contain eight characters

- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols

- User ID and passwords for staff and pupils who have left the school are

removed from the live system as soon as notified

- Enforced periodic password changes are in-built into the DLT system to enhance security

5.0   Social Media

- Individual academies within the Trust may use Facebook and Twitter to communicate with parents and carers. Relevant staff are responsible for all postings on these technologies, which are blocked for use by all students

- Individual academies are responsible for whether or not staff are permitted to access their personal social media accounts using school equipment.

- Staff are able to setup social media accounts, using an anonymous internal email address, in order to be able to teach pupils the safe and responsible use of Facebook or other applications

- Staff are not permitted to have any personal social media connection with students

- Staff should ensure that they do not publish defamatory, abusive or confidential information on their own social media accounts regarding work or about other staff.

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, governors, pupils, parents and carers must be aware that the information, comments, images and video they post on-line can be viewed by others, copied and stay online forever

- Staff, governors, pupils, parents and carers must be aware that their on-line behavior should at all times be compatible with UK law

6.0   Acceptable use agreements

- Individual academies are responsible for their own E-Safety policies at Primary and Secondary levels: ensuring they are compatible with the overall Trust Acceptable Use Policy and the DLT Staff Acceptable Use Agreement

Appendix 1   DLT Staff Acceptable Use agreement

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to be aware of the requirements of this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with your line manager or Network Manager

By indicating that you have read this policy you have agreed to the following conditions:

- I will only use the Trust's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed reasonable by the Head or Governing Body

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role

- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils

- I will only use the approved, secure e-mail system(s) for any Trust business

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the Trust's premises or accessed remotely. I will only copy data to an external storage device, such as a USB stick, in exceptional circumstances, ensuring that it is appropriately encrypted*

- I will not install any hardware or software without appropriate permission

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory

- Images of pupils, students and/ or staff will only be taken, stored and used for professional purposes in line with Trust policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Trust's network without the permission of the parent, carer, member of staff or Head teacher

- If I have been provided with a mobile phone as part of my job requirements then that phone should only be used for business purposes

- I will support the Trust's approach to online safety and not deliberately upload or add any inappropriate images, video, sounds or text that could upset any member of the Trust community

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher. I will respect copyright and intellectual property rights

- I will ensure that my online activity, both within and outside the Trust, will not bring my professional role, Academy or the Trust into disrepute

- I understand that failure to comply with this document may result in disciplinary proceedings. Please refer to the disciplinary, capability grievance and appeals policy.

There are many routes available to access central system data securely from home, such as VPN, Home Access plus or Offline files. Please speak to your local ICT technician for assistance