Langley Park Learning Trust

Acceptable IT Use by Staff Policy

Owner (job role):	Data Protection Officer
Approval Body:	Resource and Finance Committee
Approval Date:	10 December 2020
Implementation Date:	1 January 2021
Review Date:	1 January 2022

Version	Approval Date	Summary of Changes

LPLT ACCEPTABLE USE OF IT BY STAFF POLICY

Introduction

This policy is in place for use of these facilities by staff. There is a separate policy for use by pupils.

There is a small network of computers which are used in the administration of the Trust and its schools (finances, pupil records, timetables, registers etc). Many more computers are available for use by pupils and staff and the majority of these have access to the internet through the school network. All pupils and staff have a login name, password and an email account.

The email system is available for use both from within the school and externally using a web browser. There are specialist centres serving design, mathematics and science together with general purpose rooms. A growing number of other computers are located within individual departments/classroom areas.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for use of ICT by staff across the Trust.

Action plan

Each school is be responsible for ensuring that this policy is followed and therefore the school's infrastructure/network is as safe and secure as is reasonably possible. Specifically, each school must ensure that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the Trust's internal data security policy and as required by the Genera Data Protection Regulation (GDPR).
- Logs are maintained of access by users and of their actions while users of the system.
- Logs are also maintained of access under the use of personally owned ICT devices by staff policy.

The following code of practice must be adhered to by staff.

- All staff will be required to click to agree to an Acceptable Use policy when logging on.
- Staff who bring into school their own devices (BYOD), ie ICT devices not issued by the school, will also be expected to sign the BYOD usage agreement.

Rights of access

A safe and secure username/password system is essential and will apply to all school ICT systems, including email and virtual learning environment (VLE).

All passwords are generated by the network manager/ICT technical support staff and are unique to each member of staff. Passwords can only be reset by the user or by the ICT technical team. All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and these will be reviewed, at least annually.

The 'master/administrator' passwords for the school ICT system used by the network manager/ICT technical support team are also available to the headteacher or other nominated senior leaders and kept in a secure place (eg school safe). In the event of a serious security incident, the police may request, and will be allowed access to, passwords used for encryption.

Emails

The computer resources at belong to the Trust or its schools and are to be used solely for educational or business purposes, although the governors will permit limited use for personal purposes, provided that it does not interfere with work performance and provided that rules of usage are observed.

Email is an essential tool at the school and all members of staff must read and abide by the separate staff email policy when managing their email accounts, sending emails, receiving emails and especially if emailing personal, sensitive, confidential or classified information covered by the GDPR.

The Trust and its schools reserves the right to intercept, monitor, analyse and read all email generated, received or distributed via the school networks, equipment and email addresses.

Internet and intranet

Known pornographic sites on the internet are blocked and filters to intercept prohibited material and offensive language are in place. The internet is not necessarily secure and staff need to be aware that school sensitive information could be viewed by unauthorised individuals.

- Staff must abide by the current restrictions on correspondence or the passing of information to outside organisations or individuals.
- The transmission of school sensitive data over the internet is strictly prohibited.
- Devices must be locked with a password when not in use.
- At no time may staff use the internet to send school or personal information that would, if intercepted, place the school in violation of UK laws or regulations.
- Staff may not use the internet to view illegal, pornographic or seditious material that would place the school at legal risk.
- Under the government's prevent legislation, schools are required to demonstrate that they are protecting children from being drawn into terrorism. Any member of staff suspecting that pupils may be viewing or visiting suspicious websites should advise the

headteacher immediately so that the local authority (LA) can be alerted and the matter taken forward if necessary.

- Staff may not use the internet in a role inconsistent with their role in the school.
- Staff must not gain unauthorised access to the internet eg by hacking or by trying to circumvent any 'blocking' controls. Hacking into computers is a criminal offence and they could be prosecuted under the Computer Misuse Act 1990.
- Staff must not use another individual's user identity to access the internet or intranet.
- Staff may not download screensavers, sounds, images, or audio-visual materials for storage on local PCs.
- Staff may not use the internet for private business purposes or private commercial gain.
- The ordering/purchasing of goods over the internet is subject to the same authorisation procedures and limits as purchases made by other means and failure to follow the correct procedure may result in disciplinary action.
- Staff must not engage inappropriately with pupils through social networking sites. Staff must be mindful that all postings on social network sites are widely accessible. See also the social media policy.

Note. There have been many instances reported of electronic communication systems, and their output, challenging the professionalism of school staff. Colleagues should be guarded in their use of all such systems.

Delivery of remote learning

Staff may be required to deliver remote learning lessons. In this case, Microsoft Teams should be used and staff and pupils should only ever use their school email addresses to log in for home learning.

Pupils must not use their webcams when taking part in home learning.

If staff are concerned at all about delivering remote learning then they should raise this with their line manager.

Digital images

When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet, eg. on social networking sites. Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images (see the Online Safety policy). Any images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.

Portable ICT equipment

Laptops, Ipads, tablets and similar devices which are the property of the school fall under the same restrictions of use as networked computers. Serious misuse of such equipment will be treated as a

disciplinary offence and may result in dismissal. Loss, damage or theft of school equipment through misuse, or negligence may result in financial sanctions.

All school-supplied portable ICT equipment should be kept in a secure place and transported in the car boot. When not in use, they should be switched off and securely stored.

Laptops and other devices that are the personal property of the individual must only be used in line with the use of personally owned devices by staff policy.

Misuse of computer systems by staff

Misuse or abuse of computer systems by staff is a serious matter and will be dealt with under our disciplinary procedures. The penalties for improper use may include dismissal either with or without notice. The following are expressly prohibited:

- The unauthorised export or transmission of school software via the internet.
- The accessing, viewing, downloading or forwarding of pornographic material or material of a racist or inflammatory nature.
- The loading, downloading or forwarding of games software.
- The generation or forwarding of 'chain' messages or letters.
- The sending or forwarding of abusive or offensive emails – inside or outside the school – or material that could cause offence. This applies to all email, whether intended for person-to-person communication or wider distribution.

The list may be added to at any time.

Some email systems have the capability to send the contents of messages to fax machines. This policy applies equally to such messages and documents.

Any queries regarding this policy should be addressed to the headteacher.

Monitoring and evaluation

All use of the internet is recorded and the headteacher may request access to internet logs, emailing history etc if the senior management team considers that this policy has been contravened, in order to investigate alleged abuse. The policy itself will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the rolling programme of reviews by the Trust.