Langley Park Learning Trust

Acceptable IT Use by Pupils 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 PUPILS POLICY

Introduction

This policy is in place for use of ICT facilities by pupils across the Trust's schools. There is a separate policy for use by staff.

The internet provides children and young people with a wealth of opportunities for their entertainment, communication and education. But there are also risks of harm through the deliberate behaviour of others online, and through exposure to inappropriate content. The Trust and its schools have procedures in place to safeguard all learners from unlawful, sexual or otherwise potentially harmful content on the internet. Information on internet safety and the importance of monitoring internet use at home is made available to all parents annually.

There are many computers available for use by pupils and the majority of these have access to the internet through the school network. All secondary pupils 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 departments 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 pupils at our schools.

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:

- Pupils can only access data to which they have right of access.
- No pupil should be able to access another's files without permission.
- Access to personal data is securely controlled in line with the Trust's internal data security policy and as required by the General Data Protection Regulation (GDPR).
- Logs are maintained of access by pupils and of their actions while users of the system.

Rights of access – pupils

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 pupil. Passwords can only be reset by the user or by the ICT technical team. All pupils 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.

ICT code of practice – pupils

The following code of practice must be communicated to pupils by each school, and similarly worded codes of conduct signed by each pupil where appropriate:

- All pupils will click to agree to an Acceptable Use Policy that appears on screen when they first log in. The key messages of the Acceptable Use policy, to include Online Safety info guidance should also be reiterated to pupils on a regular basis. Acceptable Use messages will be appropriate to the age group of each school.

- Pupils 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.

- When not in use, devices must be locked with a password.

- The facilities are provided to support and enhance curriculum-related activities. Where required, each pupil will be issued with his/her own username and password, which must be kept confidential. Pupils must remember to log off when they have finished using the computer. It is good practice to change passwords regularly.

- Pupils must use their school login details and email addresses for school-related activity, including remote learning through Microsoft Teams.

- Pupils must never activate webcams when at home and learning remotely. Only teachers leading lessons should use webcams, at their discretion.

- Pupils must never record or video a teacher delivering a remote lesson.

- The use of another person's username and password, abusive language, sending abusive messages and changing computer settings are all serious offences.

- Pupils must not copy, alter, print or change another pupil's work in any shape or form without the person's prior knowledge and consent. Please note that copyright regulations apply to electronic publications as they do to paper.

- Pupils must use the internet and printing facilities only to support their school work.

- Pupils should be aware that information on the internet may not always be reliable and sources should be checked. Also websites are used for advertising material, which may influence the contents.

- Emails are not secure once they leave our network. Therefore, users must not share any sensitive information that could be misused if shared, or any inappropriate content that might bring the school into disrepute.

- Pupils must not disclose to anyone on the internet their home address, telephone number, the name of the school or a photograph of themselves unless specific permission is given from a member of staff. Nor should they ever arrange to meet anyone unless this is part of a school project approved by their teacher.

- Pupils must never pretend to be anything or anyone that they are not and must be aware that the posting of anonymous messages is forbidden.
- Pupils must not engage with internet chatrooms.
- Pupils must not engage with any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.
- If a pupil sees something which makes her/him feel worried or uncomfortable, s/he should report it immediately to a member of staff and never respond to bullying, suggestive or unpleasant emails or blog entries.
- Pupils must not send abusive email, chain email, excessive quantities or excessive sized emails. Nor must they use email to send or encourage material that is pornographic, illegal, offensive or invades another's privacy.
- Pupils must not vandalise the system by:
    - Physical damage.
    - Changing configuration or cabling unless specifically directed by a member of staff.
    - Hacking of the school or internal systems. Pupils should be aware that hacking into computers is a criminal offence and they could be prosecuted under the Computer Misuse Act 1990.
    - Changing the contents of the hard disks.
    - Downloading or installing software onto the network, unless written as part of an approved school computer project and with the teacher's permission.
    - Bringing food and drink into computer areas or in the vicinity of classroom computers because spillages can cause serious damage to electronic equipment.

Misuse of computer systems by pupils

- Internet and email

Please note that in the case of misuse of internet and email facilities the following action will be taken:

- First offence – the pupil will be reported to the network manager and will have access to the internet and email withdrawn for two weeks. Parents will be informed. The pupil will still have access to intranet and basic application software.
- Second offence – procedure as above but with a four week ban and a formal letter sent home to parents.
- Third offence – parents will be invited to a formal meeting with the Online Safety member of the senior leadership team, to discuss the way forward and sanctions.

- Pupils who use other pupils' accounts and access restricted file areas

These are considered to be serious offences. The network manager will record the offence and will immediately inform the year tutor of the situation. Suspension of a pupil's access to all ICT facilities will take place after the year tutor has informed the appropriate staff.

The length of the ban may vary according to circumstances but it is likely to be for at least four weeks.

To restore access, a note is required from the year tutor.

- Damage to hardware

If a pupil damages hardware, the network manager will contact the main office staff. A letter will be sent to parents. The pupil will be charged for the damage.

- Accessing websites which could be considered to support extremism, radicalisation or terrorism

If a pupil is found to engage over the internet with any organisations which could be considered to support extremism, radicalisation or terrorism of any kind then the matter will be reported to the headteacher who has a legal obligation to report it to the local authority (LA).

- Other serious offences and inappropriate use of ICT facilities

Other serious offences and inappropriate use of ICT facilities will result in the following sanctions:

- An immediate ban from the network pending investigation.
- A letter home informing parents of incorrect ICT use and a minimum ban of two weeks from the internet/email facilities.
- Subsequent offences will lead to a four to eight week ban and/or an exclusion of three days from school.
- More serious or long term abuse will lead to a total network ban and possible exclusion from school.

UNDER EXCEPTIONAL CIRCUMSTANCES, SUCH AS ABUSE WHICH MAY BE DETRIMENTAL TO THE SCHOOL NETWORK, THE NETWORK MANAGER MAY DISABLE A PUPIL'S ACCOUNT WITH IMMEDIATE EFFECT.

Monitoring and evaluation

The policy 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.