Acceptable Use of ICT Policy
2022

1.Introduction

This policy applies to all employees and contractors of Leopold Primary School. This document defines the schools policy in respect of the acceptable use of its information and communications technology facilities and the conduct of staff, contractors, governors and volunteers in relation to handling data.

2. Scope

It is the policy of school:

- to provide a working environment that encourages access to knowledge and sharing of information in a safe and controlled way
- to maintain ICT facilities for academic and administrative purposes to support our pupil's learning.

3. Principles of Use:

The activities prohibited under this policy include (but are not restricted to) those listed below. Users are required to read, understand and comply with the principles of use when utilising the school systems or acting on behalf of the school:

General Principles of Use:

Users must not:

- access, create, change, store, download or transmit material which the school may deem to be threatening, defamatory, abusive, indecent, obscene, racist or otherwise offensive.
- send unwanted or personal emails using the school's e-mail system.
- install any software that is not licensed to the school and / or install without authorisation software licensed to the school on any of the school's computer systems under any circumstances.
- use the ICT facilities for commercial or social or purposes.
- create or transmit any offensive, obscene or indecent images, data or other material and cause the reputation of the school to be undermined.

- reproduce or distribute any materials, data, pictures, files, document, video, audio produced in the schools without prior authorisation from a member of the Leadership Group or in contravention of the Data Protection Policy
- make use and possess, distribute, sell, hire or otherwise deal with any unauthorised copies of computer software for any purpose without the licence of its owner.
- allow others to gain such unauthorised access, either wilfully by disclosing user names or passwords or neglectfully by failing to log out of the system, thereby permitting unauthorised use of schools' account.
- attempt to circumvent the school's firewall systems.
- change, damage, dismantle, corrupt, or destroy any network component, equipment, software or data, or its functions or settings.
- connect any non approved computer network equipment (including wireless access points).
- share personal data of others with third party organisations (e.g learning platforms) without the permission of the Data Protection Lead and ensuring consents have been obtained where appropriate.
- fail to report a data breach related to use of the school ICT system
- delete information on the ICT system which is the subject of a 'Subject Access Request'
- Breach the retention schedule adopted by the school in relation to Data Protection.
- Breach provisions of the School Data Protection Policy - whether or not on site or using a school device, platform or network, and will ensure they do not access, attempt to access, store or share any data which they do not have express permission for.
- share credentials and immediately change passwords and notify the Data Protection Lead if they suspect a breach. Staff will only use complex passwords and not use the same password as for other systems.
- store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

Principles in relation to Remote Working

Users are expected to comply with the following:

- Support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Executive Headteacher (if by an adult).
- Refrain from behaving any differently towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- Refrain from attempting to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
- Using personal devices to access school systems or hold school information without SLT approval.
- During remote learning sessions, users are expected to:
  - Refrain from taking secret recordings or screenshots of myself or pupils during live lessons.
  - Only conduct video lessons in a professional environment. This means staff will be correctly dressed and not in a bedroom. The camera view will not include any

personal information or inappropriate objects and where possible blur or change the background.

- Refrain from contact or attempted contact of pupils or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways. Staff are expected to report any breach of this by others or attempts by pupils to do the same to the Executive Headteacher.
- Keep a log for live lessons if anything inappropriate happens or anything which could be construed in this way.
- Be aware that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
- Act as a role model and promote positive online safety and model safe, responsible and positive behaviours

Principles of social media use

Staff are required to comply with the following:

- Protect professional and organisational reputation - Your professional reputation is an essential part of your current and future career so managing your reputation online is essential. Think carefully before sharing or posting information online about the school, staff, pupils or parents – even if your account is private. Comments that are made public could be taken out of context and could be damaging to yourself and the school. The language you use is important - anything that you post online is potentially public and permanent.

- Think carefully about how you present yourself when you post images or comments; and how this may impact on the reputation and vision of the school. Please ensure your online profile is highly professional, appropriate for pupils to see and does not bring the school into disrepute. An employer may reasonably believe that a recognisable member of staff putting an inappropriate post, image or making comments in the public domain will lower the reputation of the school and this could be a basis for disciplinary action. It is an implicit condition of employment that an employee owes a duty of loyalty to an employer.

- Choose your networks carefully - Think carefully about who you connect with online and who can access information about you. The school requires that you do not accept friend requests, or requests to follow you, on your personal accounts from pupils, past or present, or from parents at your school. By accepting such requests, you would be making yourself vulnerable by sharing personal information or by having access to personal information about pupils. This would leave you open to allegations of inappropriate contact or conduct and you could find yourself exposed to unwanted contact.

- Privacy settings - It is a good idea to customise the privacy settings, if access to your personal activity could compromise your position. It is important, regardless of which setting you use, that you think about what you post because ‘friends’ settings do not guarantee privacy. Be careful about comments you post - sharing content with others could mean that you lose control of it.

- Your professional responsibilities - Please remember that if you put out information about the school, school staff, pupils or parents in the public domain, you will be held to account for it. It can be deemed to constitute gross misconduct which could lead to dismissal. Staff are must ensure they comply with the duty not to promote partisan political views.

4. Prevention, Detection & Investigation of Misuse

The school reserves the right to monitor from time to time any data that is stored on a user's account and any e-mails passing through the school network to minimise the risk of misuse of the ICT facilities.

5. Confirmation

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's GDPR and safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____
Name: _____
Role: _____
Date: _____