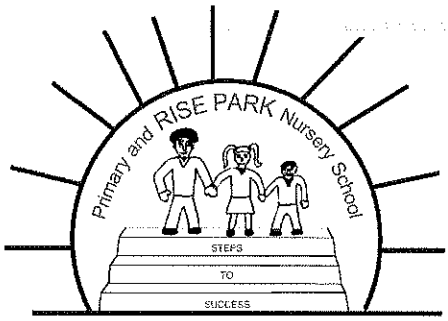

General Data Protection Regulation (GDPR)

Rise Park Primary and Nursery School Acceptable Use Policy

June 2018

Signed by Chair of Committee	
Print Name	J Kinloch
Date	2.7.18
Date of review	

Acceptable Use Policy

1. Introduction

Rise Park Primary and Nursery School ('the school') Acceptable Use Policy does not aim to impose unreasonable restrictions. The school is committed to protecting its employees, partners and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing and FTP are the property of the school. These systems are to be used for business purposes in serving the interests of the school and of the school's pupils, families and staff in the course of the school's normal operations.

Ensuring effective security of the school's network is a joint effort involving the participation and support of every school employee and any associated colleagues who deal with school information and/or information systems. It is the responsibility of every computer user to be aware of these guidelines and to organise their work accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the school. These rules are in place to protect both employees and the school itself. Inappropriate use exposes the school to unacceptable risks including virus attacks, compromised network systems and possible legal challenge.

3. Scope

This policy applies to the use of information, electronic and computing devices and network resources to conduct school business, or interact with internal networks and business systems, whether owned or leased by the school, a school employee or a third party. All employees, contractors, consultants, temporary and other workers at the school (and its subsidiaries, linked schools, etc.) are responsible for exercising good judgment in relation to appropriate use of information, electronic devices and network resources in accordance with school policies and processes as well as the law and relevant codes of practice.

This policy applies to employees, contractors, consultants, temporary and other workers at the school, including personnel affiliated to third parties.

4. Policy

General Use and Ownership

Employees must use extreme caution when opening e-mail attachments received from unknown senders as they may contain malware.

5. Unacceptable Use

The following activities are generally prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the school authorised to engage in any activity that is illegal under local bye laws, national law or international law while using school-owned or leased resources.

The lists below are not exhaustive, but try to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities.

The following activities are strictly prohibited, with no exceptions:

- Damage to the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of copied or other software products that are not appropriately licensed for use by school.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and the installation of any copyrighted software for which school or the end user does not have an active license is prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using school computing assets to actively engage in procuring or transmitting material that is in violation of harassment and/or other workplace regulations.
- Making fraudulent offers of products, items or services originating from any school account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of

an employee's regular work duties. Blogging and use of social media from the school's systems is also subject to monitoring.

- The school's approach towards confidential information also applies to blogging and social media. As such, employees are prohibited from revealing any of the school's confidential or protected information, or any other material considered to be confidential by the school when engaged in blogging or accessing social media.
- Employees shall not engage in any blogging or use of social media that may harm or damage the reputation and/or goodwill of school and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by school's policy around non-discrimination and anti-harassment.
- Employees may also not attribute personal statements, opinions or beliefs to the school when engaged in blogging or social media. If an employee is expressing his or her beliefs and/or opinions, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the school. Employees assume all risk associated with blogging use of social media.
- Apart from following all laws applying to the handling and disclosure of copyrighted materials, the school's trademarks, logos and any other school intellectual property may also not be used in connection with any blogging or social media activity.

6. Policy compliance measurement

The school's Headteacher will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits and feedback from employees.

7. Exceptions

Any exception to the policy must be approved and recorded by the school's Headteacher.

8. Non-compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9. Related policies and processes

- Data Protection Policy
- Email Policy
- Internet Use Policy
- Social Media Policy
- Password Policy

This page is intentionally blank