Management of Information Policy

Our aim is to provide the foundations for a positive future for our pupils.
A future where pupils learn to stay safe, to understand the importance of a healthy lifestyle , and to enjoy all they do.
A future where they are money smart & make a positive & respectful contribution to their culturally diverse community – at a local, national & global level.

A future where they aspire to be the best they can be & achieve their full potential.

Created ……2015……To be reviewed 2018
Signed C of Gov……..
Headteacher……..

Policy for the Management of Information in School

The school will be aware of and comply with all Current Data Protection Legislation in effect.

Ownership of the Management Process will rest with the Headteacher who is responsible for ensuring that all aspects of Data Management are dealt with in accordance with this policy.

All Data pertaining to the school will be held on the school administrative computer [or network] and will be password protected. Access to the data will be password protected and only the Headteacher, their Deputy and the School Administrator shall have access.

Passwords should be changed once a month to ensure security and where possible should contain upper and lower case letters mixed with numbers and the length of the password should be greater than six characters.

Input of Data is the responsibility of the School Administrator who should ensure that all data pertaining to the school is input in an accurate and correct manner. [However it may be that a clerical assistant can have limited access to enable low level data input]

The production of reports based on School Data is the responsibility of the Headteacher, the Deputy Headteacher and the Administrator, depending upon the nature of the report. Reports may take the form of printouts or electronic media for transfer via post or e-mail. All reasonable steps will be taken to ensure security of such information.

Any removable media used to transfer or hold data must be encrypted/password protected and all reasonable steps taken to ensure security of such media

If Data is stored on a school laptop it must be securely encrypted/password protected to guard against unauthorised and illegal access.

Where e-mail is used to transfer data, security measures must be maintained, and systems for password protection of mail accounts must be adhered to. All users with access to school mail systems should have secure passwords and are responsible for ensuring that their own security is maintained.

Reports are produced for a variety of audiences, such as Governors, Staff, Parents, LA and National Government, and transfer schools, and are confidential to their intended audience.

Reports and information once printed remain confidential and Governors and staff should be aware of basic security to ensure that data and information is not accessed by unauthorised persons.

Provision of Authorised Information to Government bodies, LA and other schools in the form of PLASC Census, Attendance Data, LA Census and requests, and School transfers etc. is the responsibility of the Administration officer and ultimately the Headteacher to ensure requests are met.

Where legitimate requests for information are made to the school then the school will endeavour to comply with such requests within 5 working days or within request deadlines when set by Local and National Government.

Ringway AppleID & iCloud Security

IPads require an Apple ID and the use of an iCloud account to interact with the iTunes store and save to a cloud workspace where files can be access on another device.

1. Pupils

The following descriptors apply to the pupils at Ringway Primary school.

1.1 Apple ID for students under 13:

For students under 13, Apple IDs and iCloud are requested by the school or school district and then created upon receipt by Apple of verifiable consent from a parent or guardian. These accounts must be created by the parent or guardian on behalf of the student. They must not be used as a personal account. Apple IDs for students under 13 have limited targeted advertising, and by default, iCloud email is not activated. Staff should not create accounts for students nor should they allow use or creation of Apple ID for students. If an account is created by parents with a signed agreement, which should be obtained and stored safely within the school, then students can use the Apple ID to:

- Receive app licenses and redeem codes for education books and textbooks.
- Take notes in iBooks and sync those notes between iOS devices, such as a school-owned iPad. Pupils should not sync their school Apple ID to a personal Apple ID.
- Enroll in iTunes U courses.
- Download education content again, if needed for the next school year.

The iCloud should only be used by the students as a means of educational data storage with the intent of accessing, sharing and editing content on other school-owned devices.

1.2 Apple ID security measurements for users under 13:

If an Apple ID is created, under the descriptors above, Apple will automatically set the following security measures on the account:

- Account settings, such as email address and date of birth, cannot be changed.
- No credit card is attached to the account at setup.
- Targeted advertising will be limited.
- Accounts are unable to opt in to receive marketing materials from Apple.
- Parents or guardians are notified by email of material changes to the service or issues with the account.

If an account password is entered incorrectly three times the Apple ID will automatically lock. Staff members should not create a new password: instead parents should manage the account and should be notified of any changes to the account.

1.3 Student privacy

When students use an Apple ID or the iCloud [in relation to 1.1 of this document] they must confirm to the Apple privacy policy and staff will ensure this is adhered to during use. This policy is publicly available on the Apple website: apple.com/privacy. A further guide for parents can also be found at apple.com/education/docs/Apple_ID_Parent_Guide.pdf.

2. Staff use:

2.1 Use of Apple ID and the iCloud

Staff should not use a personal Apple ID nor should they access the iCloud using their personal details. Instead, accounts should be created for purposes of education. Staff should be aware of legal and copyright issues relating to the use of the internet, iCloud and apps while using the Apple devices. The IT coordinator at the school should manage the educational accounts and have access to them.

2.2 Security

1. If a password is incorrectly entered three times the account will be locked and a new password must be set by the staff member on a web browser. Any changes to the account information must be notified to the schools IT coordinator.
2. The iCloud only allows access to photos through shared iDevices or a desktop computer with the iCloud sync app. Photos which are taken and uploaded to the cloud should adhere to the schools e-safety policy. If a desktop is used, rather than an iDevice, staff members should ensure the desktop computer is a secure school computer which has an antivirus and a firewall active.

2.3 Access of information

Staff must ensure that they, and their pupils, access and distribute appropriate content. They must refer to the e-safety policy for legal, moral and ethical guidance in relation to accessing and sharing content through the schools Apple devices and use of the educational Apple ID's and iCloud.

Icloud is secure and two-factor authentication is added security so if this is in place then there should be no issues raised about security.

This policy was adopted by the Governing Body on _____/_____/_____

It is due for revue on _____/_____/_____