NORTHBURN
PRIMARY SCHOOL

ACCEPTABLE USE POLICY

Document #: ECS_AUP_0716

EMAIL & CLOUD STORAGE

July 2016/ Reviewed July 2017

It is the responsibility of the school to ensure all staff curriculum network users sign, print and date this document, then return it to the school administration team. The school is responsible for retaining such information for the purpose of audit reviews.

The school are using Microsoft Office 365 to provide hosted email and cloud storage for all curriculum staff.

The purpose of this Policy is to describe the procedures and processes in place to ensure the safe and secure use of the organisations Office 365 Email and OneDrive facility, its users, and to protect the organisation systems and data from unauthorised access or disclosure.

This Policy document has been provided by the organisations IT Support Representative; Subrideo. This document does in no way associate itself with the organisations admin email facility. The admin facility is governed by the local authority.

Any queries arising from this Policy or its implementation, can be taken up directly with the school head teacher, or IT Support Representative: info@subrideo.co.uk

Summary of Contents:

1 Foreword

i. Email are subject to disclosure rules and rights of access by individuals as provided by the Data Protection Act. This means that accounts 'held' within Office 365, can be accessed and searched by the organisation in order to comply with legislation. All staff should ensure appropriate language is used to maintain the professional standards required by the organisation. All information must reflect the organisations code of standards, i.e. polite, contain no exclusionary language and adhere to any policy the organisation may have for equal opportunities.

ii. The civil and criminal legislation relating to written communication applies to e-mail messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, libel, harassment, wrongful discrimination, Data Protection Act, Official Secrets Act and Criminal Procedures and Investigation Act. Staff must not enter anything in an e-mail that you would not write on paper – all accounts are auditable.

2 Violations of Office 365 Email

i. Consideration must be given where confidential and/or sensitive information is included in an email. For example, if personal information is included, there should be guidance as to how this e-mail is to be disposed of, e.g. ‘not for forwarding to any other persons’.

ii. Staff should ensure that they review messages at least once a working day and delete those of a sensitive nature as soon as they are no longer required.

iii. In the event of sending photographs as email attachments, staff must ensure they adhere to the organisations photograph policy, and ensure that a standard parental permission has been obtained.

iv. Every member of staff in the organisation must set the permission for their immediate line manager and at least one other supervisor to review their Inbox.

v. When on annual leave you should always select the 'Out of Office' reply.

vi. Important messages that need to be retained should be saved in a folder in the user's personal home drive or within a shared area on the network.

vii. Do not send other peoples personal information, or any commercially sensitive information, via email unless encrypted. Please use Message Encryption within Office 365. If you are unsure of how to use this facility, please consult with the IT Administrator.

viii. Staff are responsible for managing their email records in the same way that they are responsible for managing other business records. Each member of staff has a set mailbox quota of 50GB, for storage of emails. If you exceed the maximum quota for your mailbox, you will be unable to send or receive emails.

ix. Deleted Items should not be used as a file store. Emails deleted from your Deleted Items folder will recoverable for up to a 14-day period, after this period they will be permanently deleted.

x. The use of PST files for archiving is not an acceptable means of retaining information.

xi. Computers connected to organisations network must not be left unattended and running e-mail. This will leave your e-mail account open to misuse.

xii. Staff working from home must not leave personal computers unattended and running email. This will leave your email account open to misuse. Staff must ensure home computers used for work use, have separate user profiles in place and that only the staff member has access to their computer profile.

xiii. The e-mail system is provided for primarily business use.

xiv. Internal chain letters must not be used and are forbidden within the organisation.

xv. Messages sent via e-mail can be forwarded to other users without the originator's knowledge or permission; users should take into account the originator's view before forwarding e-mails which have been sent to them.

xvi. Each user must maintain a tidy inbox, deleting any old or unwanted messages on a regular basis

xvii. Target messages to only those who need it.

xviii. Do not assume that a message has been read (ask for confirmation/or use the receipts function).

Violations of Office 365 OneDrive

i. Staff must ensure no files are downloaded to an external device outside of the organisation network. Users must only use Word Online, Excel Online and PowerPoint Online, provided within Office 365 OneDrive for Business. Alternatively a locally installed instance of Word, Excel or PowerPoint, can be used to access the file, providing the users follows the OneDrive for Business instruction guide. This instructs the user on connecting the locally installed Word, Excel or PowerPoint to the cloud storage facility. Both methods ensure the file(s) are always retained within the OneDrive storage area, and not downloaded to the local device.

ii. Staff should ensure that they review their OneDrive areas and delete files once no longer required in their cloud storage area.

iii. Staff are responsible for managing files/ folders in their OneDrive storage areas, in the same way that they are responsible for managing other business records.

iv. Staff should not use the OneDrive storage as has their primary storage facility.

v. Staff must ensure the primary storage area is their personal network area on the organisation file server. The organisation takes no responsibility for the loss of data from within the OneDrive platform.

vi. Staff must ensure they do not share any files or folders in their OneDrive area with an external body. Shared content is only permitted with other organisation users.

vii. In the event of storing photographs in OneDrive for Business, staff must ensure they adhere to the organisations photograph policy, and ensure that a standard parental permission has been obtained.

viii. The storage of copyright material is not permitted in a user's OneDrive area.

ix. Computers connected to organisations network must not be left unattended when a user has left their OneDrive session active.

x. The OneDrive for Business system is provided for primarily business use.

xi. Each user must maintain a tidy OneDrive area, deleting any old or unwanted messages on a regular basis.

4 Passwords

i. Passwords must be used in order to access computers, applications, systems and all other networked resources

ii. Passwords must meet complexity requirements; alpha-numeric, contain eight or more characters of which at least one must be a digit.

iii. Passwords must not be proper names, address names or birth dates. Network login / user names must not be used in any form (reversed, capitalised, or doubled as a password).

iv. The same password must not be used for more than one application, system, device or service.

5 Mobile Devices

i. Mobile devices are not permitted for use with the organisations email platform.

ii. Any mobile device added to the platform, will automatically be placed into quarantine.

6 Audit and Review

i. ICT and information security is managed through the IT support contractor, school head teacher, school ICT coordinator, school administrative team and school governing body. ICT and information security is subject to regular audit and review.