Acceptable Use Policy
For the Internet and Electronic Mail

Consultation with Staff: Sep 18

Adopted by Governing Body: 01.10.18

Review date: Annually

1. Introduction.
This document sets out the terms and conditions under which users will:

- Access the Internet
- Make use of resources information on the Internet
- Disseminate information via and arising out of the Internet
- Communicate using the Internet

This document applies to all staff to whom the internet is available via accounts set up by the school and includes both networked and stand-alone computers within school with access to the Internet.

2. Warning against Deliberate Misuse of the Internet
The Internet is a valuable resource. It also presents significant dangers to the School from staff or visitors who may choose to abuse it. Whilst each case will be judged on its own merits, the following warning is issued to all staff:

(a). Any member of staff who commits a breach of any School Policy, regulation or Standing Order as a result of unauthorised use of the Internet (including electronic mail) will be subject to the sanctions listed in the Online Safety Policy. Staff needing clarification on policies, should consult the head teacher. Additionally:

(b). If the School discovers that a member of staff or visitor has committed a criminal offence or has been party to the commission of one as a result of unauthorised use of the Internet, the Police will be contacted immediately,

(c). The School will in no way indemnify a member of staff or visitor who has incurred any liability as a result of unauthorised use of the Internet. The School will seek financial redress from members of staff or a visitor whose unauthorised use of the Internet causes the School to suffer a loss.

3. Protection of staff acting in good faith
It is fully recognised that a member of staff or visitor may accidentally breach this Policy whilst acting in good faith and in the course of their duties as a member of staff or visitor of the School. If a member of staff or visitor suspects this to be the case, they MUST notify the head teacher/ Online Safety Lead IMMEDIATELY so that action can be taken to prevent or minimise damage.

4. Unauthorised uses of the Internet

- The copying of software files from the internet should be kept to a minimum. No executable files should be copied from the internet. Software downloads must only be carried out by a member of staff who is capable of ensuring that it is not faulty, is not infected with a virus and that all copyright requirements are met. If there is any doubt, the ICT co-ordinator or network manager should be contacted.
- Do not access any site that involves any form of gambling or betting,
- Do not open a subscription account on the Internet on behalf of the School without express permission of the head teacher,
- Do not leave PCs in a state where it would be possible for someone other than the normal user (or other legitimate user) to access the Internet,
- Do not leave your PC unattended whilst it is on the Internet.
- Do not publish personal information or information relating to the school community on social networking sites.

It is the responsibility of all users to report any unauthorised acts to the Head teacher. Additionally, users are requested to follow the principles of good practice set out below:

Internet

- Do not reveal your own (or any other person's) personal details eg. home address, telephone number over the Internet,

Electronic Mail

- Electronic mail is not a person-to-person communication, always use appropriate language.
- Never use electronic mail to send or forward chain letters or any material which may contravene School policies (e.g. jokes, pictures of a racist, extremist or sexist nature)
- At least once a week, ensure that all unwanted electronic mail messages are deleted from the INBOX, Sent and Trash folders.
- Check your mailboxes regularly, at least once a day.

Mobile phones

- Do not use personal mobile phones in the presence of pupils or to take photographs on the school premises
- Do not use personal Ipads or mobile phones to take photographs of pupils on trips

5. Reviewing this Policy

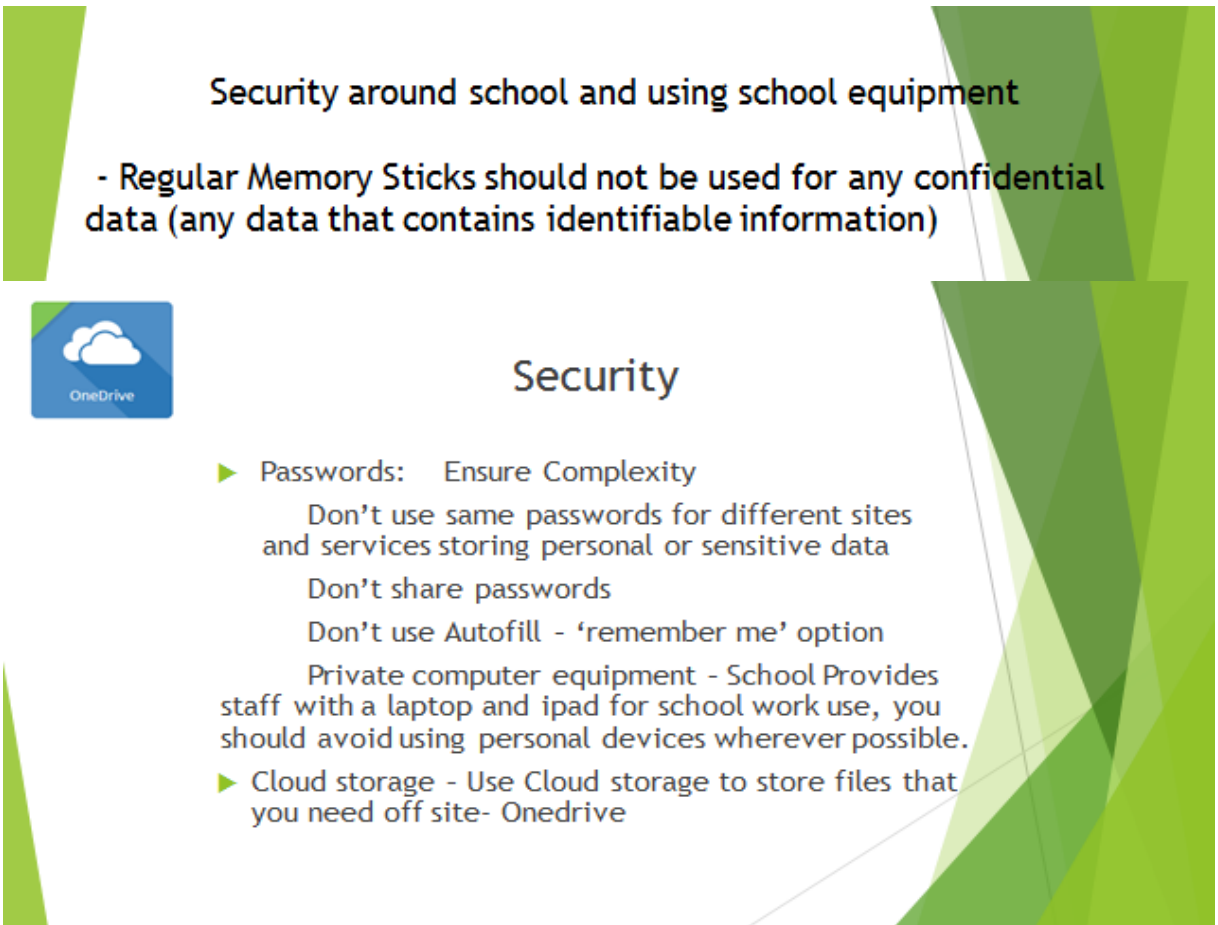
This Policy will be reviewed and re-issued at least annually as the use of the Internet develops.

6. Member of Staff signature

I have read the School's acceptable use of the Internet policy and accept that it forms part of my conditions of employment.

Employee's Name _____ Employee's Signature:_____

GDPR UPDATE – May 2018



E-mail Security

Use BCC when emailing a group of people in order to keep their contact details private; Ensure that the body of the email doesn't give away personal or sensitive information;

Don't forward emails to a personal account that contain personal or sensitive attachments;

Use official school email accounts as opposed to personal email accounts

Don't send emails from personal addresses

- the computer has an up to date virus checker to avoid a malicious piece of software gaining access to user names and passwords;
- individual users are set up on the device;
- the computer is only used to access data held in secure storage, whether it be in the cloud, through remote access or from an encrypted memory stick;
- at no time should Personal Data be stored on the devices unencrypted memory or hard drive;
- when processing Personal Data this is completed in a secure area away from other family members;

If staff access school email through a personal mobile phone and/or tablet:

- they must PIN protect any device used to access their work email;
- they must make sure that their device is safe and secure at all times;
- they must never send Personal Data through accounts that have not been provided by the school
- They must sign out of any work related system as soon as they are done.