HR22

OLD BUCKENHAM HALL

Brettenham Park
Ipswich, Suffolk, IP7 7PH
Website: www.obh.co.uk

Acceptable Use of ICT, Mobile Phones & Social Networking Policy

(Employees, Peripatetics and Visitors)

April 2015

OLD BUCKENHAM HALL

Acceptable Use of ICT and Mobile Phones Policy
(Employees, Peripatetics and Visitors)

PURPOSE
The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and mobile phones for employees, peripatetics and visitors to OBH. Its purpose is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to ICT systems.

This policy deals with the use of ICT facilities at OBH and applies to all employees and other authorised users, e.g. peripatetics and volunteers.

This Policy applies to all staff, visitors and Peripatetics including the Pre Prep and EYFS

SCHOOL RESPONSIBILITIES
The Governing Body and Headmaster are responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

The Head of ICT is responsible for maintaining an inventory of ICT equipment and a list of school laptops and mobile phones and to whom they have been issued.

If a member of staff, peripatetic or volunteer has reason to believe that any ICT equipment has been misused, he/she should inform the Headmaster or the Business Manager. The investigation of the allegations/ Incidents will be investigated in a timely manner in accordance with agreed procedures.

Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment.

Staff are required to read this policy and to confirm they have read and understood it. This may be done by e-mail or writing to the Business Manager

USER RESPONSIBILITIES

- Users must report all suspected breaches of this policy to the Headmaster or Business Manager.
- Users and their line managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.
- By logging on to ICT systems, users agree to abide by this Acceptable Use policy and other policies that relate to the use of ICT.

- All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.
- Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed for under *Personal Use and Privacy* below
- Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite.
- No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the School.
- Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.
- No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.
- Users must not load or download software on any device without the authorisation of the Head of ICT. Periodic audits of software held on ICT equipment will be undertaken.
- Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops.
- Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.
- No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.
- Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

    a. There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.

b. An account appears to be engaged in unusual or unusually excessive activity.
c. It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability.
d. Establishing the existence of facts relevant to the business.
e. Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities
f. Preventing or detecting crime
g. Investigating or detecting unauthorised use of ICT facilities
h. Ensuring effective operation of ICT facilities
i. Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
j. It is otherwise permitted or required by law.

- Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.
- Websites should not be created on school equipment without the written permission of the Head of IT.
- No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.
- The following content should not be created or accessed on ICT equipment at any time:

  a. Pornography and "top-shelf" adult content
  b. Material that gratuitously displays images of violence, injury or death
  c. Material that is likely to lead to the harassment of others
  d. Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age
  e. Material relating to criminal activity, for example buying and selling illegal drugs
  f. Material relating to any other unlawful activity e.g. breach of copyright
  g. Material that may generate security risks and encourage computer misuse

- It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headmaster and Head of IT. This may avoid problems later should monitoring systems be alerted to the content.

PERSONAL USE & PRIVACY

In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users

subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs. Lunchtime use is considered the user's own time.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.

Personal use of the Internet must not involve attempting to access the categories of content that is normally automatically blocked by web filtering software.

MOBILE PHONES AND INSTANT MESSAGING

- Mobile Phones should be switched off and not used during work time.
- At no time are mobile phones to be used in the Pre Prep & EYFS departments.
- Staff are advised not to give their home telephone number or their mobile phone number to pupils.
- Photographs and videos of pupils should not be taken with mobile phones.
- Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils, text messages other than for approved school business.
- Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework.
- Staff should not enter into instant messaging communications with pupils.

SAFE USE OF SOCIAL NETWORKS (eg:FACEBOOK)

- The School takes a serious view and does not permit friendships with pupils at OBH or ex pupils under the age of 18 years
- Staff must consider carefully their use of social networks and take full responsibility for anything on their page with regard to the reputation of OBH and themselves as professionals
- Staff should protect themselves by doing the following:
    a. No messages should be written which has any mention of school business (work, pupils, activities)
    b. No photographs should be posted of staff, pupils or school events
    c. Privacy should be set at the highest level to limit users to your page

MONTIORING AND REVIEW

This policy will be monitored by the Headmaster, Head of ICT and Business Manager. The policy will be reviewed annually by the Head of ICT and the designated Governor.

A. Shropshire
Business manager

Oct 2013
Amended Apr 2015