OLD BUCKENHAM HALL

A leading co-educational preparatory school for children aged 2-13 years

Acceptable Use of ICT, Mobile Phones and Social Networking Policy for STAFF

OBHP08

Policy owner: Head of ICT
Date of issue: October 2021
Date last reviewed: October 2021
Next review due: October 2022

ACCEPTABLE USE OF ICT AND MOBILE PHONES POLICY
(Employees, Peripatetic staff 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 applies to the use of:

- all internet and electronic mail facilities, computers (including tablet and smartphones), and any networks connecting them provided by the School;
- all hardware owned, leased, rented or otherwise provided by a member of staff and connected to or otherwise accessing School networks or other facilities;

This Policy applies to the entire school, including 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 ICT Technician and the Head of ICT (in the event of there being no technician) 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 Head of ICT or the Director of Finance and Operations. 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 Assistant Bursar.

This policy should be read in conjunction with the following documents:

- Data Protection Policy
- e-Safety Policy
- Acceptable Use Contracts for pupils.

User Responsibilities

- Users must report all suspected breaches of this policy to the Headmaster, the Director of Finance and Operations or Head of ICT.

- 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 General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. 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.

- Personal material – especially music and pictures – should not be stored on the school system.

- 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. For their own protection, users must ensure that they log off or lock their machines when leaving them unattended.

- No user shall access (e.g., read, write, modify, delete, copy, move) another user's 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. USB memory sticks are not to be used for school data unless they are Bitlocker encrypted - and then only with the express permission of the Head of ICT. Please see the ICT Technician if you are not certain. Please note that all school laptops issued to staff have SSDs encrypted by Bitlocker.

- School data – e.g. pupil / staff names and contact details should not be stored on personal devices. Where a school device is not available, personal devices may be used to access school email or iSAMS. Such personal devices should be password protected and, preferably, should be remotely erasable if lost. School data should not be stored on personal devices – for example, email attachments received should be deleted or saved onto your school OneDrive for Business once they have been viewed. Teaching staff using personal devices to write reports should either type them directly into the School's MIS or, if using a program such as Word to prepare them, ensure that they are saved on the school OneDrive. Staff using a device connected to the school's network via VPN should ensure that data is only saved on the school network. The ICT staff can provide advice.

- iSAMS, the school's MIS, is set up so that both the email and the export pupil data functions are only available to staff logging on at school (the school's ip address is trusted) or via the school VPN. Two factor authentication is needed for those usings iSAMS off site.

- Personal devices connected to the school network in any way must have school approved anti-virus software installed and activated. 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 school 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. Please note that it is possible to send secure emails from the school system by starting the title with the text 'Securemessage' – please see the ICT Technician / Head of ICT for further information.

- Websites should not be created on school equipment without the written permission of the Head of ICT.

- 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 ICT. This may avoid problems later should monitoring systems be alerted to the content.

Remote Teaching

As a result of the COVID-19 pandemic, the school was completely closed from March-June 2020 and teaching was online using Microsoft Teams. It is possible that the system will be used again—either partially or completely—in the event of further measures. It is also envisaged that pupils or teachers who are absent from school for a different reasons will, in the future, make use of the system.

The following guidelines apply:

- Safeguarding is of paramount importance. Children are encouraged in the AUPs that they should contact a trusted adult if they have any concerns about anything online and any staff with safeguarding concerns should report these to the DSL or Alternates. They should also be recorded in the CPOMS system, links to which are found on the intranet.

- Only software authorised by the school should be used and teaching staff should use their school laptops whenever possible. All staff and pupils have Microsoft 365 accounts and only this system should be used for communicating with pupils. (Zoom is also permitted – please see below.)

- Video teaching material should be uploaded and run from Microsoft Stream whenever possible as only those with a school 365 account can view. The school YouTube channels are used for some material, but, for reasons of privacy, staff are advised to ensure that teaching videos are 'unlisted' and are removed when no longer needed.

- All live remote teaching sessions using MS Teams or Zoom should be recorded and kept on the school system for one calendar month before deletion.

- In live sessions, teachers need to be smartly dressed and should choose an appropriate background. Students should also be appropriately dressed and sitting at a table / desk.

- In the event of online teaching, parents will be informed that there may be links to YouTube videos. Teachers must ensure that all video resources referenced in their teaching material are suitable and age appropriate.

- Teachers having any queries should direct them to the Deputy Head Academic or the Director of Studies.

Personal Use & Privacy

In the course of normal operations, the OBH ICT resources are to be used for school 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.

Please be aware that school email accounts should not be used for personal emails of a confidential nature. If a member of staff leaves, or is absent for an extended period, it may be necessary to arrange for their email accounts to be accessed by another member of staff in order to ensure the smooth running of their department. Any such redirection will be performed by the ICT Technician at the request of a member of the Senior Management Team.
For all staff, logins to school systems will cease upon termination of their contract of employment.

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 Messaging (by any form)

- Mobile Phones should not used during work time.
- At no time are mobile phones to be used in the Pre-Prep & EYFS departments. Staff in these departments must leave their mobile devices in the staff room during working hours.
- Staff must not give their home telephone number or their mobile phone number to pupils.
- Photographs and videos of pupils must not be taken with personal devices but only on school equipment.
- Staff must not use pupils' mobile phone numbers for any reason. Staff needing to contact a pupil urgently, must do so via parents / guardians (and see below)
- Staff should only communicate electronically with pupils from school accounts (e.g. the school email system, iSAMS or the VLE) on approved school business, e.g. coursework, prep, holiday revision.
- Staff should not enter into any other form of messaging communication with pupils.
- The iSAMS app may be installed on a personal device. Access to this requires two-factor authentication and all devices on which the app is installed are recorded by the system and activity is logged. Data from the app must not be copied.

Safe Use of Social Networks (eg Instagram, Facebook)

- The School does not permit friendships with pupils at OBH or ex pupils under the age of 18 years. This should also apply to staff who leave the employment of OBH. Be aware that such social networking friendships can be misinterpreted and lead to allegations being made.
- 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 have 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

Monitoring and Review

This policy will be monitored by the Headmaster, the Director of Finance and Operations, and the Head of ICT. The policy will be reviewed annually by the Head of ICT in conjunction with the Director of Finance and Operations.