OLD BUCKENHAM HALL

E Safety Policy

February 2015

OLD BUCKENHAM HALL

E-Safety Policy

Introduction

Technologies are constantly changing and therefore any policy needs to be as dynamic as possible and in constant review. The school needs to be sufficiently flexible to manage new and emerging technologies, as they may have important educational and social benefits. The policy aims to balance the use of existing and emerging technologies with the necessity of providing safeguards for pupils and employees against risks and unacceptable material and activities.

This Policy considers devices used by pupils and includes those that may have been provided by the school (such as PCs, laptops) and those technologies owned by pupils, but brought onto school premises (such as kindles, laptops, mobile phones).

Although children may be trusted by their parents with regard to private internet use, the school has a duty to safeguard them. Parents need to be reassured that their child is not able to access material deemed unsuitable and/or in contravention of the School's Acceptable Use Agreement. This policy applies to all pupils, with any concessions for boarders being detailed.

The existence of the many and various forms of electronic devices and equipment, in any environment, raises issues of security and personal responsibility, not only in terms of its appropriate use but also for its safe keeping. The School does not accept responsibility for, nor is insured against theft, loss or damage of any pupils' personal property, including electronic devices.

Areas of risk (Ref Ofsted 2013)

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content,
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership - such as music and film)

Procedures and Practices

The school provides pupils and staff with Internet access and access to the school's own network through connections across the site. Pupils and staff have an individual username and password with the means to create and save files on the school network. All pupils and staff have a private area on the network which can only be accessed using their particular logon credentials.

The school's internet access is provided by Skyline Networks Ltd and is filtered on site using the latest BLOXX device and a Sophos UTM.

'Safe search' for Google, etc. is enforced on site for pupils / staff on both wired and wireless sections of the network.

All domain logons are filtered for internet access by the BLOXX system, with different levels for pupils and staff. A summary of what is filtered is attached as an appendix to this policy. At present any non-domain logons – for example mobile phones, iPads – are filtered by our Sophos UTM. It is intended that all access will eventually be routed through the BLOXX device for ease of operation / monitoring.

Pupil use of devices such as e-readers, tablets and mobile phones is strictly controlled via the mobile devices policy. It should be noted that pupils are not allowed mobile phones which could access the internet independently of the school's ICT systems.

Pupils are asked to read and initial the school's acceptable use agreement on an annual basis.

E-Safety Roles

Headmaster / SMT

- Assume overall responsibility for e-safety
- Ensure that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- Are aware of procedures to be followed in the event of a serious e-safety incident.
- Receive regular reports from the E-Safety Lead

E-Safety Lead & Head of ICT (Mr Chris Bunting)

- Takes day to day responsibility for e-safety issues and has a co-ordinator / leading role in establishing and reviewing the school e-safety policy
- Promotes an awareness and commitment to e-safeguarding throughout the school community
- Ensures that e-safety education is embedded across the curriculum.
- Liaises with school ICT staff
- Reports to the HM / SMT / DSL to discuss current issues, report and review any incidents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Ensures that an e-safety incident log is kept up to date
- Facilitates training and advice for all staff
- Facilitates workshops / discussion groups with parents

Head of ICT in conjunction with ICT Staff

- To report any e-safety related issues that arises, to the E-Safety Lead.
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)
- To ensure the security of the school ICT system
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices

- To ensure that web filtering devices are maintained and and updated on a regular basis
- Ensure that they keep up-to-date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- To ensure that the use of the school's network / Moodle VLE / remote access /email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Lead / SMT for investigation / action / sanction
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

All Staff

- To embed e-safety issues in all aspects of the curriculum and other school activities
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To read, understand and help promote the school's e-safety policies and guidance
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- To report any suspected misuse or problem to the E-safety Lead
- To maintain an awareness of current e-safety issues and guidance e.g. through CPD
- To set a safe, responsible and professional example in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Parents

- To support the school in promoting e-safety
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To consult with the school if they have any concerns about their children's use of technology
- To attend where possible any workshops that have been organised by Old Buckenham Hall about any issues relating to e-safety.

Pupils

- To read and understand the Acceptable Use Policy for pupils.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

Pupil Agreement for safe and appropriate use of ICT facilities

Every pupil at OBH is asked to read the following document giving rules for responsible use of the ICT facilities. This document is discussed in Forms and ICT lessons to ensure that pupils understand why these rules are to be used.

Rules for Responsible Computer Use

The school has installed computers with internet access to aid pupils' learning. There is also an email system which you can use to contact your friends and family.
These rules will help keep you safe and be fair in your behaviour towards others. They also cover the use of e-mail and the computers in general.
We have tried to keep these rules as simple as possible so that everyone can understand them.

Using the Computers

- ***If I am worried about anything I find on the computers I will tell a teacher.***
- *I will only access the computer system using the username and password I have been given.*
- *I will not give my username and password to anyone else.*
- *I will use the computers sensibly and not interfere with any of the wiring or the settings of the computers. When I have finished I will leave the computer tidy for the next person.*
- *I will not attempt to access others' files.*
- *I will not bring in CDs, DVDs or USB drives from outside school and try to use them on the school computers without permission from Mr Bunting or Mr Chinnery. All memory sticks should be registered with Mr Bunting or Mr Chinnery and a list is kept in the ICT Office. If permission is given, then these disks are for work purposes only and should not to be used for bringing in games.*
- *I will use the computers according to the timetable displayed throughout the school. I understand that the computers are provided primarily for work and I will not use them for games at Break. Games may be played in the evening if the duty staff allow access to the ICT Room.*
- *I understand that deliberate misuse of the computers may result in action being taken.*

Using the Internet

- *If I see anything or receive any messages I do not like, I will tell a teacher immediately because this will help protect other pupils and me.*
- *I will not deliberately search for inappropriate material on the internet.*
- *I understand that all my use of the internet is recorded and that the ICT staff may check my computer files and the sites that I visit.*
- *I will not give away any personal information to any sites on the internet. If I am not sure about this, I will ask a teacher.*
- *I will not download any files or applications without permission from Mr Bunting or Mr Chinnery, except images to be used in class or project work.*
- *I will not use any chat rooms.*
- *I will not copy work from the internet and claim it as my own.*

Using e-mail

- *I will only use the OBH e-mail system (unless given permission from Mr Bunting) as other email cannot be policed.*
- *I will not give my email password to anyone else nor will I try to use someone else's account.*
- *Messages I send will be polite and reasonable.*
- *If I receive any emails that I am worried about or that I find unpleasant, I will tell a teacher as soon as possible.*
- *I will only e-mail people I know, or that my teacher has approved. For my own safety I will not give any personal details such as my email address, home address or phone number to people or organisations that I do not know.*
- *I will not use the email system to send games or inappropriate material to other people.*

Remember that these rules are for your own safety.
If you are concerned about anything, tell a teacher.
The 'Internet Safety' button on the home page of the School Intranet links to the CEOP website.
I confirm that I have read and understand this policy.

……..

Restrictions for pupils

- Pupils may only use the school email system. Web mail (eg Hotmail) is blocked.
- Chat Rooms and social networking sites are blocked.
- Gambling and E-Commerce are blocked.
- Other blocked categories include pornographic, hate and discrimination, violence, drugs, offensive and tasteless, newsgroups and forums, media streaming / downloading

Concessions

- The use of suitable/age appropriate games of a non-educational purpose is allowed after 7p.m except those games which involve or incite violence or involve a repetitive use of keys in a rigorous manner which may damage the equipment
- The use of Skype is permitted for certain overseas pupils (with permission from boarding staff) in order to contact their families.

Measures in place to support the policy:

The Acceptable Use Policy protects all parties by clearly stating what is acceptable and what is not. This is discussed and explained with all pupils, initialled and then kept in a file within the ICT department.

Education

All pupils joining the school receive ICT lessons. A key component of these lessons is to achieve an understanding of the important issues of e-safety contained within this policy. We not only look at what is acceptable/unacceptable behaviour, but we also discuss the consequences of these actions. Material is age-appropriate and most of the content is based on the CEOP recommendations.

Whole Staff

It is the responsibility of the ***whole*** staff to be vigilant at all times, not just specific members of staff. This includes trips out, residential trips, break times, lessons, and after school. We regularly remind staff of the need for this duty.

Parents

The school is keen to educate parents/guardians and our aim is to organise regular workshops, sessions etc. This is a crucial link to helping keeping children safe, as issues can occur when pupils are at home and not using the school systems.

Other

Assemblies, workshops, PSHE lessons and form groups all address cyber-bullying, safe use of the Internet and appropriate use of technologies.

Monitoring and Sanctions

The school will exercise its right to monitor the use of computer systems, including the monitoring of internet use, including the email system, and the deletion of inappropriate materials at all times. In circumstances where the school believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the school reserves the right to inform appropriate authorities and provide documentary evidence. The computer network is owned by the school and may be used by pupils to advance and extend their knowledge and understanding.

Pupils should be aware that computer/mobile phone memory, e-mails and other forms of electronic information storage and communication (including any external storage media which pupils bring into the School) may be scrutinised for the purposes of safeguarding or promoting a child's welfare. This would normally be authorised by the Headmaster, Deputy Head or SMT.

Although all staff and pupils are expected to use ICT responsibly and receive specific education to define and encourage responsible use, the school recognises that it has a responsibility to counter any

attempts at irresponsible behaviour which may still arise. The School's ICT system is monitored and managed in a number of ways designed to inhibit abuses, specifically:

Web Filtering – the School subscribes to reputable services (Bloxx / Sophos) that maintains an on-line database that categorises websites. Some categories are banned permanently, some are restricted to adults only. The databases of the filtering devices are updated on a daily basis.

Mail Filtering – Incoming and outgoing Junk and 'spam' emails, and also any containing malware are filtered out.

Computer Logs – all user logon and logoff activity is logged. All website requests are logged and users are taught this.

Social Networking sites – access to these is blocked for pupils.

Expectations of Pupils and Parents beyond the School

When a pupil is at home, families bear responsibility for the guidance of their children. The school expects the use of ICT by its pupils, even when at home, to comply with the school's stated ethos. Material downloaded in the home, posted in cyber-space from a home computer, or transmitted to a mobile phone when a pupil is at home, can impact significantly upon the life of pupils at school. Thus we ask all parents/guardians to cooperate with the School in the education of their children in the use of ICT.

Most initial offences will be dealt with by the Head of ICT / e-Safety Lead and the removal of computer access may result. In such circumstances parents/guardians may be notified. The incident will be recorded in the e-safety log.

More serious offences or repeated abuse of ICT by a pupil will be dealt with by the Headmaster in conjunction with the Head of ICT / e-Safety Lead. The removal of computer access may result and other sanctions may also be applied. In such circumstances the pupil's parents/guardians will be notified and may be asked to come into school.

Under circumstances when abuses of ICT constitute a safeguarding concern the Designated Safeguarding Lead will take appropriate action.

Monitoring and Review

This policy is monitored on a daily basis by all staff but especially the Head of IT. It will be reviewed as a result of an incident, changes in guidance, or on an annual basis.

Chris Bunting
Head of ICT February 2015