HITCHIN BOYS' SCHOOL
An Academy Trust

Policy Title:	**E-Safety Policy**
Date adopted:	April 2020
Review Date (Term & Year)	May 2021
Governors Committee:	Resources Committee
Staff member leading:	Ry

Introduction

ICT is an essential resource in the 21st Century in supporting teaching and learning as well as playing an important role in the everyday lives of young people. The school recognises the responsibility to educate students on e-safety issues and to equip them with the skills needed to use these technologies appropriately. We are also aware that there are risks and dangers associated with their inappropriate use.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

This policy is designed to support staff in their use of technology and help to ensure effective and safe pupil use of the Internet and other technologies.

This policy aims to set out what constitutes safe and acceptable use of the Internet and other electronic and digital services. It has regard to the DCSF Guidance *Safe to Learn: Embedding anti-bullying work in schools* and advice issued by the Local Safeguarding Children Board (LSCB). It relates to other policies and documents including those for Acceptable Usage, Safeguarding and Child Protection, Anti Bullying, Discipline and PSHE.

We endeavour to embed e-safety messages across the curriculum whenever the Internet and/or related technologies are used.

Internet Access

Why is Internet use important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration system.

How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries.
- Access to websites which provide students with extra practice and manage staff workload by marking students answers.
- Educational and cultural exchanges between pupils world-wide.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues; improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with external agencies – such as examination boards and DfE.
- Communication with parents through email, social media and apps.

How will Internet use enhance learning?

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide students in online activities that will support the learning outcomes planned for the student's age and maturity.
- Pupils at Key Stage Three and Four will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Our use of Google allows resources to be shared and edited, homework to be recorded and questions set and marked.

How will students learn to evaluate Internet content?

- Pupils will be taught that if they discover unsuitable sites, the URL (address) and content should be reported to the Network Manager in the first instance, so that appropriate steps can be taken. (Reported to Hertfordshire Internet and connectivity services, who investigate the site). Pupils should be taught to be critically aware of the materials they read on the Internet and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will email be managed?

- The use of email within the school is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private.
- All members of staff and pupils have their own email account for all school business. It is the responsibility of each account holder to keep the password secure. Staff should not contact pupils or parents using their personal email addresses. Emails created or received for work will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff email accounts should be used as follows:

- Emails should be checked regularly.
- Emails of short term value should be deleted.
- School email should only be used for School communication
- Staff must inform the Network Manager if they receive an offensive email.
- School policies apply whether school email is accessed in school or remotely.

Pupils will be informed that:

- They may only use approved email accounts on the school system.
- They must immediately tell a member of staff if they receive offensive email.
- They must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Excessive social email use can interfere with learning and may be restricted.
- Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

- **How should Website content be managed?**
- The point of contact on the Website should be the school address, school email and telephone number. Staff or pupils home information will not be published.
- Written permission from parents or carers will be obtained when a pupil joins the school to allow photographs of pupils to be published on the school website.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- The school will respond to all incidents of cyberbullying and will follow the procedures laid down in the anti-bullying policy.

How can the Internet be managed?

In common with other media, such as magazines, books and video, some material available via the Internet is unsuitable for young people. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school cannot accept liability for the material accessed.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

The School will:

- Regularly review the methods used to identify, assess and minimise risks associated with Internet use.
- Examine emerging technologies for educational benefit and monitor for potential threats.
- Ensure that staff and pupils are aware of this policy.
- School uses the HICS web filtering service.

How will Internet access be authorised?

Parents will be asked to sign and return a form stating that they have read and understood the Acceptable Usage document.

Safe use of Images

The school seeks the written consent of parents (on behalf of pupils) when they join the school, to permit the use of their child's work/photos in the following ways:

- on the school website;
- in the school prospectus and other printed publications that the school may use for promotional purposes recorded/transmitted on a video;
- in general media appearances e.g. local/national media/press releases sent to the press highlighting an activity;

This consent form is considered valid for the entire period that the pupil is at school, unless there is a change in the child's circumstances where consent could be an issue e.g. divorce of parents, custody issues. Parents may withdraw their permission in writing at any time. The school also seeks permission as part of the trips process for the use of images from that trip. When images are taken the purpose of them should be explained to the student.

Members of staff should not usually use personal digital equipment, such as mobile phones and cameras, to store and record images of pupils. The school can provide such equipment for trips, outings and other events.

CCTV

The school uses CCTV for security and safety and follows the ICO CCTV Code of Practice guidance (https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/). People with access to this are members of the SMT, Heads of Year and the IT Department**.**

Personal Mobile Devices (including mobile phones)

- Pupils must not use their mobile phones during the school day without permission from a member of staff and the school takes no responsibility for the loss, damage or theft of any personal mobile device if brought to school.
- Staff must not make telephone contact with parents using their personal mobile phones, but should use school equipment for such contact, except in the case of an emergency.

School Mobile Phones

The School has a number of mobile phones which are available for staff to use on trips. These are kept in the School Office and should be booked with the School Trip Secretary. Phones should be returned to the School Office as soon as the trip returns to school.

How will the policy be introduced to students?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be taught through the ICT programme, covering both school and home use.

How will staff be consulted?

- All members of staff are governed by the terms of the Acceptable Usage Policy in school
- All staff, including teachers, supply staff, classroom assistants and support staff, will be provided with the School e-safety Policy, via the Staff Handbook.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data

Protection Act 2018; The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998, Sexual Offences Act 2003; Racial and Religious Hatred Act 2006 and Police and Justice Act 2006.

- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

How will ICT system security be maintained?

- The school ICT systems are reviewed regularly with regard to security.
- Virus and firewall protection is installed and updated regularly.
- Unapproved system utilities and executable files will not be allowed in pupils work areas or attached to email.
- The network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to the Designated Safeguarding Lead.
- Any complaint about staff misuse must be referred to the Headteacher.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. Sanctions available include:

    - interview/counselling;
    - informing parents or carers;
    - removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

Some issues, although involving e-safety, may be more wide ranging. In these cases, the sanctions may be more severe and other disciplinary procedures will be followed.

How will parents' support be enlisted?

It is essential for parents/guardians to be fully involved with promoting E-safety, both inside and outside of school. We seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents' attention is drawn to the Acceptable Usage Policy for pupils, the school Web site and 'parent workshops'.
- Parents are encouraged to contact the School Office, who will advise the relevant member of the Pastoral Team, if they have any concerns regarding E-safety issues.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

Pupils with additional needs

The school endeavours to send a consistent message to pupils, parents and staff with regard to e-safety. Some pupils may require additional teaching, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Appendix 1

References

Particularly for Parents and Children

Bullying Online www.bullying.co.uk

Advice for children, parents and schools

FKBKO - For Kids By Kids Online www.fkbko.co.uk

Excellent Internet savvy for kids; KS1 to KS3

Kidsmart www.kidsmart.org.uk

An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? www.thinkuknow.co.uk/

Home Office site for students and parents explaining Internet dangers and how to stay in control.

Safekids www.safekids.com

Family guide to making Internet safe, fun and productive

Particularly for Schools

NAACE / BCS www.naace.co.uk/publications

A guide for schools prepared by the BCS Schools Committee

and the National Association of Advisers for Computer Education (NAACE)

Internet Watch Foundation - www.iwf.org.uk

Invites users to report illegal Web sites

Child Exploitation & Online Protection Centre **www.ceop.police.uk**

e-Safety in Schools **www.kenttrustweb.org.uk/esafety**

Appendix 2

Copyright

Notes on the legal framework

This page must not be taken as advice on legal issues, but the following legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following application to the Headmistress. The Acceptable Usage Policy, which every user must agree to, contains a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

Data Protection Act 2018 concerns date on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

The Telecommunications Act 1996 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1999

Obscene Publications Act 1959 and 1964 defines "obscene" and related offences.

The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;

- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

APPENDIX 3

ICT Systems: Acceptable Use / eSafety Rules Policy

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will only use my school email account for school related communication only. I will **not** give out my school email address to any persons/organisations who/that are not connected directly with the school without permission from the school.
- I will only use online accounts that have been set up by/for me for all online services.
- I will not download or install software on school equipment.
- I will not transfer any files that have been acquired illegally, including music, onto school equipment.
- I will only log onto the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone.
- I will make sure that all ICT communication with pupils, teachers or others is responsible and sensible.
- I will not deliberately browser, download, upload or forward material that could be considered offensive or illegal.
- I will not give out any personal information such as my name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I am aware that if I take images of pupil and/or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved, including in school breaks, trips and all occasions when you are in school uniform or when otherwise representing the school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute including distress caused by uploads of images, video, sounds or texts.
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.

These rules are designed to keep you and your data safe. All your use of the Internet and other related technologies can be monitored and logged and can be made available to your teachers. If these rules are not followed, school sanctions will be applied and your parent/carer may be contacted.

Signed by Pupil: _____ Date: _____

Signed by Parent/Carer/Guardian: _____ Date: _____