# HINCHINGBROOKE SCHOOL

***Inspiring Excellence  Fulfilling Potential  Developing Character***

Policy Statement
on

# E-SAFETY
# FOR STAFF AND STUDENTS

| | |
|---|---|
| Revised: | Every 3 Years |
| Date approved by Governing Body: | February 2019 (D&W Committee) |

**Part of the ACES Academies Trust**

## Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games content (not age appropriate)
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music, video or games files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically, Anti-Bullying[1], Behaviour[2], Safeguarding & Child Protection[3], ICT Acceptable Use (Staff and Student versions)[4] and BYOD[5].

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

## Scope

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

### Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy.

### Principal & Senior Leadership Team (SLT)

The Principal is responsible for ensuring:

- ✓ The safety of all members of the school community, although the day-to-day responsibility for e-safety may be delegated to senior staff and/or other appropriate staff.
- ✓ Adequate training is provided
- ✓ Effective monitoring systems are set up
- ✓ That relevant procedure in the event of an e-safety allegation are known and understood.
- ✓ Establishing and reviewing the school e-safety policies and documents.
- ✓ The school's Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

### ICT Services Manager (IT Network Manager)

The ICT Services Manager is responsible for ensuring that:

- ✓ The school's ICT infrastructure is secure and meets e-safety technical requirements
- ✓ The school's password policy is adhered to
- ✓ The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- ✓ Co-ordinator keeps up to date with e-safety technical information
- ✓ The use of the school's ICT infrastructure (network, remote access, e-mail, etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to SLT for investigation/action/sanction.

### Teaching & Support Staff

In addition to elements covered in the Staff Acceptable Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- ✓ They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- ✓ They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- ✓ E-safety issues are embedded in all aspects of the curriculum and other school activities
- ✓ Students understand and follow the school's e-safety and acceptable usage policies
- ✓ They monitor ICT activity in lessons, extracurricular and extended school activities

- ✓ In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

## Students (to an age appropriate level)

Students are expected to have an understanding of the importance of staying safe online through engagement with the school's curriculum relating to e-safety. Students should understand the associated risks of being online and act responsibly to reduce those risks. Students are responsible for ensuring that:

- ✓ They are using the school's ICT systems in accordance with the Student Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature. This is signed electronically when initially logging onto the school network.
- ✓ They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- ✓ They 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 also covers their actions out of school, if related to their membership of the school.

## Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Emphasis is now upon managing any risk rather than blocking or stopping children's use of the internet. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. This therefore requires parents/carers/adults to have a knowledge and understanding sufficient enough to discuss the risks with their children, plan appropriate boundaries and minimise and understand the risks of being on line. The school will take opportunities to help parents understand these issues and ask parents/carers to be responsible for:

- ✓ Endorsing (by signature) the Student Acceptable Usage Policy.
- ✓ Accessing the school website in accordance with the relevant school Acceptable Usage Policy.
- ✓ Monitoring the online access of their children whilst not in school.

## Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to read and understand the user acceptable use policy.

## Education and Training

**E-safety education** will be provided in the following ways:

- ✓ E-safety is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- ✓ Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- ✓ Students are helped to understand the need for the Student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- ✓ Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- ✓ Rules for the use of ICT systems and the Internet are posted in school
- ✓ Staff act as good role models in their use of ICT, the Internet and mobile devices.

## ICT Acceptable Usage Policy for Staff & Students[4]

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- **Staff and regular visitors** to the school have an AUP that they must read through and sign to indicate understanding of the rules.

## Staff Training

- The ICT Services Manager and/or DSL ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme and as part of safeguarding training, ensuring that they fully understand the school's E-Safety policy, Acceptable Usage and Safeguarding Policies.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection/safeguarding.

## Communication

### Email

- Digital communications with pupils (e-mail, online chat, voice etc.) should be on a professional level and only carried out using official school systems (see staff guidance in Safeguarding Policy).
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems) or Outlook;
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

### Mobile Phones

- **School** mobile phones only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.
- **Staff** should not be using personal mobile phones in school during working hours when in contact with children.
- **Students** should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

### Social Networking Sites

Staff and students are expected to use social networking sites responsibly and respectfully and to use these to publicise, inform and communicate information. The school has an active website and twitter account which are used to inform, publicise school events and celebrate and share the achievement of students

- **Staff** should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Students/Parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- The school will intervene where misuse of social media by students occurs outside of school and this impacts upon the day to day running of the school community. Advice may be sought from relevant external agencies, including the police, in cases of misuse of social media.

### Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list can also be obtained from the data office.
- Under normal circumstances, images of students should be taken on school equipment. Where the use of personal devices is necessitated, images should be transferred to the school network and deleted from the personal device without delay.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity. Staff should not hold images of students on personal devices.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

### Removable Data Storage Devices

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before being run, opened or copied/moved on to local/network hard disks.
- In accordance with the acceptable use policy, school data should only be stored on portable devices in exceptional circumstances and in such instances the device must be encrypted to prevent unauthorised access.

## Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.
- Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.
- The school deploys software to control and monitor internet and application usage. The ICT Services Manager and the DSL will use the software logs as part of any investigation into misuse,

## Passwords: Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 6 weeks
- Staff should take reasonable steps to use a complex password (inclusive of letters, numerical values and symbols)
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

## Passwords: Students

- Should only let school staff know their in-school passwords if requested.
- Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow students to change passwords through Impero.

## Use of Own Equipment

- Privately owned computers will not be connected to the school's network. Privately owned computers can only be connected to the school's BYOD wireless network.
- ICT equipment brought on to the school site is done so at the student and parent's risk. The school does not accept any liability for damage or loss of any privately-owned equipment.

## Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment.
- Personal or sensitive data (belonging to the school) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Windows + L) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

## Incident Reporting

Any e-safety incidents must immediately be reported to the Principal (if a member of staff) or the ICT Services Manager, Head of Year, Head of Dept. or SLT (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

## Responding to incidents of misuse

Any e-safety incident must immediately be reported to the ICT Services Manager and DSL who will investigate further following e-safety and safeguarding policies and guidance. The Principal will be informed.

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials, the appropriate reporting should be made through the school's safeguarding procedures (using My Concern or a Nagging Doubt, green form). Actions will be followed in accordance with the Safeguarding Policy, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.