Ivanhoe College

A Specialist Technology Academy

E-SAFETY POLICY

ADOPTED BY THE CURRICULUM & LEARNING COMMITTEE OF
IVANHOE SPECIALIST TECHNOLOGY ACADEMY

Date: 26th February 2020

'Journey to Excellence'

E-Safety Policy

To be Read in conjunction with
Safeguarding, Prevent, Data Protection,
Staff ICT Acceptable Use and Student ICT Acceptable Use Policies.

1. Introduction

- The underlying principles of this policy reflect the three offences outlined in the computer misuse act 1990 which are;
  - unauthorised access to computer material.
  - unauthorised access with intent to commit or facilitate commission of further offences.
  - unauthorised modification of computer material.

- Ivanhoe College recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. More than any other mode of technology, the Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

- Hand in hand with the College's desire for its students to access every opportunity for learning, there will be the need to keep them safe from the perils of the Internet, digital and mobile technologies.

- Ivanhoe College, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled children and young people increased access to the curriculum and other aspects related to learning.

- Ivanhoe College is committed to ensuring that **all** students will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with students; as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding children and young people.

For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

2. Scope of Policy

Ivanhoe College will seek to ensure that across the College the following elements will be in place as part of its safeguarding responsibilities to students:

- a list of authorised person(s) dealing with child protection issues and E-safety;
- a range of policies including authorised usage policies that are frequently reviewed and updated;
- information to parents that highlights safe practice when using the Internet and other digital technologies in school and at home;
- adequate training for staff and volunteers;
- adequate supervision of children and young people when using the Internet and digital technologies;
- education of children and young people about how to use the Internet and digital technologies safely;
- a reporting procedure for abuse and misuse by children, young people and adults.

3. Policies and Practices

Use of Internet facilities, mobile and digital technologies

This policy aims to ensure that the Internet, mobile and digital technologies are used effectively for their intended educational and recreational purposes, without infringing legal requirements or creating unnecessary risk.

- Users in the college shall not:
  Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

  - Indecent images of children
  - Promoting discrimination of any kind
  - Promoting racial or religious hatred
  - Promoting illegal acts
  - Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material.

- The College recognises that in certain planned curricular activities, access to otherwise considered inappropriate sites may be beneficial for educational use. In such circumstances, such access should be pre-planned and recorded and also permission is given by senior leaders, so that the action can be justified, if queries are raised later.

- Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the designated office for child protection within the setting and the Police:

    - Indecent images inclusive of abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
    - Adult material that potentially breaches the Obscene Publications Act in the UK
    - Criminally racist or anti-religious material
    - Violence and bomb making
    - Illegal taking or promotion of drugs
    - Software piracy
    - Other criminal activity

<u>In addition, users may not:</u>

- Use the college facilities (connectivity and services) or an equivalent for running a private business;
- Enter into any personal transaction that involves the College's information technology;
- Visit sites that might be defamatory or incur liability on the part of the College
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- The transmission of unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Deliberate unauthorised access to facilities or services accessible via the college's network,
- Deliberate activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end
    - systems accessible via the college network and the effort of staff
    - involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;

- using the College network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- continuing to use an item of networking software or hardware after the College has requested that use cease because it is causing disruption to the correct functioning of the network;
- other misuse of the network, such as introduction of viruses.
- Use mobile technologies 3G or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

3.2 Reporting abuse

- There will be occasions when either a pupil or an adult within the College receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation is that the student or adult should report the incident immediately.
- The College also recognises that there will be occasions where children and young people will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances Leicestershire Safeguarding Childrens Board (LSCB) Procedures should be followed. The expected response will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the setting refer details of the incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.
- The College, as part of their safeguarding duties and responsibilities will, in accordance with LSCB Procedures, assist and provide information and advice in support of child protection enquiries and criminal investigations.

4. Education and Training

- The College is committed to harnessing the power of the Internet and other digital technologies to transform the learning of children and young people. We are also dedicated to ensuring that students have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

- As part of achieving the above, the College will seek to ensure that E-safety training is made available to children, young people; and also to those adults that supervise them, manage and/or support the facilities that are being used e.g. network managers, technicians, administrators as well as third party service providers.

5. Sanctions

- The College has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable establishments to manage such situations with confidence.

- Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

Student

The student will be disciplined according to the behaviour policy of the college, which will ultimately include the use of Internet and email being withdrawn.

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy.

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.