E-SAFETY POLICY

E-safety encompasses internet technologies and electronic communications. It highlights the need to provide ongoing education to children, young people, staff and the community (including parents and carers) about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

It is vital that the users, staff and students are protected from potential harm that may be considered an e-safety issue.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Anti-Bullying and Curriculum, Safeguarding, the Acceptable Use Policy (AUP) and Social Media. All staff and students are responsible for E-safety at Heart of England School. Our E-safety policy and its implementation will be regularly reviewed.

SAFE AND RESPONSIBLE USE – STUDENTS AND STAFF

- The School's e-Safety policy is available for inspection at any time.
- All computer use on networked computers will be monitored and is traceable
- Monitoring of activities using our wifi access for students is implemented as far as it is practicable.
- The awareness and importance of safe and responsible use of electronic communications will be emphasised and supported via an E-Safety training programme which will be regularly reviewed.

SOCIAL MEDIA – STUDENTS AND STAFF

- This is covered in the Social Media Policy.

MANAGING E-MAIL

- This is covered in the AUP

MANAGING 'PUSH' COMMUNICATIONS SUCH AS TWITTER

- This includes ALL the policies named at the top of this policy
- Ensure your postings are subject related, topical and only refer to students by their school usernames
- Use caution with hashtags – they could link to inappropriate material
- Inform the Communications Manager of all usernames and passwords

MANAGING USE OF THE INTERNET AND MATERIAL RESOURCED FROM IT

- Internet access is available for students who show a responsible and mature approach to its use. The access can be removed if necessary.
- The school will advise that the copying and subsequent use of Internet derived materials by staff and students should follow copyright law as per the AUP. Students will be encouraged to be critically aware of the materials they read and advised to validate information before accepting its accuracy. They will be shown how to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- If staff or pupils discover unsuitable sites, the URL (address) must be reported to ITHelpdesk immediately.

SUPPORTING E-COMMUNICATION

- Social networking sites and newsgroups are blocked at school unless a specific use is approved.
- Students are given education and support regarding their personal use of social networking. The current advice is:
    - **Never give out personal details** which may identify them or their location e.g.real name, address, mobile or landline phone numbers, school, IM address, social media "handle" for other media, e-mail address, names of friends, age, specific interests and clubs etc.
    - When using **educational social networking** sites **must use** the school email address as the school's monitoring system adds a layer of protection and your teacher can monitor your progress
    - **Not to place personal photos or thoughts** on any social network space. Consider how public the information is and consider using private areas; **or don't publish at all.**
    - **Think about the background detail** in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
    - **Always set a secure password and consider security** especially on public and unsecured networks. Be aware of security at all times
    - **Deny access to unknown individuals**. Only let your friends be part of your network.
    - **Never meet up with a person you have only 'met' online** unless you have permission from an adult parent/carer. Ensure you are accompanied by that adult when meeting.
    - **Block unwanted communications**.
    - **The school does not resolve bullying conflicts which happen outside the school**. During the course of the school day, mobile phones should neither be seen nor heard. There are students who are granted certain privileges with regards to mobile phones during social time (see the Behaviour Policy). Bullying on the school's network is covered in the AUP and the Behaviour Policy. If the issue is significant the parents/carers should consider contacting the police.
- Teachers' official blogs or wikis must be password protected and associated with their school email address.

MANAGING THE SCHOOL'S WEBSITE

- The contact details on the website will be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.
- E-mail addresses should be published carefully to avoid spam harvesting.
- The Principal or Vice Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

PUBLISHING IMAGES / MEDIA OF STAFF AND PUPILS

- All Images / Media of students and staff will be stored on a dedicated networked drive.
- Photographs on websites that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the school website, particularly in association with photographs, unless requested by the student concerned for professional reasons.
- Permission from parents or carers will be checked before photographs of students are published on the school website.
- Students' work can only be published with the permission of the student.
- Images of staff should not be published without verbal consent.

MANAGING IT SYSTEMS SECURITY

- School IT systems capacity and security will be reviewed by Solihull Council using six monthly penetration testing and by the school's Network Manager when any security flaws are identified either internally or externally.
- Virus protection will be installed and updated regularly by both Solihull Council and Heart of England School.
- The school maintains specialist software for the management of e- safety which is explained clearly in the Acceptable Use Policies and which monitors computer-based activities.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

MANAGING FILTERING

- The school's technicians will work to ensure current best practice for filtering and monitoring systems are as effective as possible; they must remain aware of the need to ensure that filtering policies take account of new developments on the Internet.
- If staff or pupils discover unsuitable sites the URL must be reported to the school's IT Helpdesk and where appropriate a taupe 'Concern Form' must be completed.
- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is considered.
- The school should regularly review its policy on phone use in the light of emerging technologies.

PROTECTING PERSONAL DATA

- Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act (2018) and the General Data Protection Regulations.

E-SAFETY COMPLAINTS

- Formal complaints of Internet misuse using the school systems will be dealt with by a senior member of staff.
- Any complaints about staff misuse must be referred to the Principal who should use the agreed SMBC procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

COMMUNITY USE OF ICT AND THE INTERNET

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and co-operate with external bodies (e.g. police) if necessary.