Spring Hill High School

Student ICT Acceptable Use Policy

Policy: ICT Acceptable Use Policy
Procedure Reference: SHHS/TOO 1
Version Number: 1.0
Date : May 2016
Review Date: September 2017
Authorised by: Directors and Responsible Individual(RI)
Updated by: Fawzi Ahmed
To be read in conjunction with: E Safety Policy and Safeguarding Policy

Context: The Acceptable Use Policy at Spring Hill High School covers the security and usage of all information and ICT equipment. This also includes the use of email, internet, voice and mobile equipment. This policy applies to all students.

Aim: Our aim is to ensure that students at Spring Hill High School use ICT effectively, safely and responsibly without infringing legal requirements or creating risk.

All use should be consistent with Thoughts Of Others Ltd policies and practice.

1.0 **Monitoring:** All computer usage within Spring Hill High School is fully monitored at all times by teachers, Learning Support Assistants (LSAs) and authorised ICT staff who may inspect ICT equipment owned by the school. These inspections can take place at anytime without prior notice.
1.1 ICT authorised staff will monitor, intercept, access, record and disclose telephone calls, emails, instant messaging, Internet use and any other electronic communication (data, voice, video or images) involving its students without consent. This maybe to confirm or investigate compliance with school policies, standards and procedures and to ensure the effective operation of school ICT.
1.2 Students will be provided with guidance by staff in the use of the resources available through the school's network. School staff will regularly monitor the classroom environment to ensure that it is being used responsibly

2.0 **Breaches:** A breach or suspected breach of policy by a student may lead to:

- Temporary or permanent withdrawal of the school's ICT hardware, software or services from the offending student.
- Reporting the student's actions to parents/ carers /guardian and, in extreme cases, the police.
- Reporting student's actions to the safeguarding officer where a safeguarding issue has been identified.
- Close monitoring and supervision of the student's network activity by teaching staff, Learning Support Assistants (LSAs) and the school's ICT authorised staff.

3.0 **Incident Reporting:** Any security breaches or suspected misuse of ICT must be immediately reported to one of the school's Deputy Headteachers, Assistant Deputy Headteacher, Headteacher or Directors.

4.0 **Conditions of Use**
Student access to the networked resources is a privilege, not a right.

4.1 Students will be expected to use the resources for the educational purposes for which they are provided.

4.2 It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Students must also accept personal responsibility for reporting any misuse of the network to the Data Protection Officer, Chris Delahaye, or a member of staff.

4.3 Use of any information obtained via the network is at the student's own risk.

Acceptable Use Agreement

Students are expected to use the network systems in a responsible manner.
Examples about what is, and what is not, acceptable are provided below.

1	I will not attempt to communicate with any other student via my mobile device whilst in school e.g. social networks, instant messaging, telephone calls.
2	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 through uploads of images, video, sounds or texts.
3	I will not create, send, or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
4	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
5	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
6	I realise that files held on the school computers will be regularly checked by members of staff.
7	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
8	I will not trespass into other users' files or folders.
9	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
10	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact a member of staff.
11	If I find an unattended machine logged on under other users' username I will **not** continue using the machine – I will log it off immediately.
12	I understand that there is no access to social networks in school.
13	I will not use the internet to access any material that relates to the promotion of extremism or terrorism.
14	I will only access academic research material involving defamatory, discriminatory or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material under the supervision of the teaching staff or LSA.
15	I will not use the computers in any way that would disrupt use of the computers by others.
16	I will report any accidental access to other people's information, unsuitable websites, or being sent inappropriate materials that make me feel uncomfortable, to a member of staff.
17	I will not introduce "USB drives" or other portable devices into the computer without having them checked for viruses.
18	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
19	I will not download and/or install any unapproved software, system utilities or resources from the Internet.
20	I realise that students under reasonable suspicion of misuse in terms of time, activity or

	content may have their usage closely monitored or have their past use investigated.
21	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
22	I will not attempt to harm or destroy any equipment, work of another user on the school computer, or even another website or network connected to the school system.
23	I will not attempt to access the network on personal mobile devices. If I connect accidentally it should be reported immediately to a member of staff or the ICT department.
24	I will not access any material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.

Unacceptable Use
Examples of unacceptable use include, but are not limited to:

- Creating, transmitting, displaying or publishing any material (text, images or sounds) that is likely to harass, cause offence, inconvenience or needless anxiety to any other person
- Unauthorised access to data and resources on the school computers that belong to other "users".
- User action that would cause:
    - Corruption or destruction of other users' data,
    - Violating the privacy or dignity of other users,
    - Intentionally wasting time or resources on the school computers or elsewhere.

Network Security
If you discover a security problem, for example being able to access other user's data, you must inform a member of staff immediately and not show it to other users. Students identified as a security risk will be denied access to the computers.

Student User Agreement Form for the Student Acceptable Use Policy

I agree to follow the school rules on the use of the school network resources. I will use the computers in a responsible way and observe all the conditions explained in the school Acceptable Use Policy complying with the policies of Thoughts of Others Ltd.

I agree to report any misuse of the network and report any websites that are available on the school Internet that contain inappropriate material to a member of staff.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that all usage of computers is fully monitored.

Student Name: _____

Student Signature: _____

Parent /Carers/Guardians Name: _____

Parent /Carers/Guardians Signature: _____

Date: __/__ /_____

The school will not be responsible for any loss of data as a result of the system or student's mistakes in using the system.