Spring Hill High School (TOO)
Acceptable Use Policy for Telephone, Email and Internet Use.

Policy: Acceptable Use Policy (for Staff)
Procedure Reference: SHHS/TOO
Version Number: 1.0
Date : June 2017
Reviewed Date: June 2018 by Chris Delahaye
Review Date: June 2019
Authorised by: Directors and Acting Responsible Individual(RI)
Updated by: Sheraine Reid-Ferguson
To be read in conjunction with: Anti-Bullying Policy, Staff Disciplinary Process and Procedure

Introduction

1.1 The use of the internet is one of the most popular source of information for employees at Spring Hill High School. Ease of use and speed has also made email the most common form of communication among employees within the organisation. When used correctly, the internet and email provides an efficient way of sharing information.

1.2 Taking pictures and videos of the student's achievements and activities is a wonderful way of capturing a memory and promoting successes but consideration needs to be given to who might have access to the images.

1.3 The reality we face is that our students are at risk of abuse or exploitation through advances in technology. Spring Hill High School is committed to protecting and safeguarding all children and young people in our care to ensure as much as possible that they stay safe.

1.4 Section 11 of the Children Act 2004 place an obligation on us all to safeguard and promote the welfare of children and young people. The Data Protection Act 1998 also emphasises the need to ensure that appropriate consent is given for the use of images of clearly identifiable people, children and adults alike.

1.5 The increased use of technology has made it easier to use pictures and images in either print or web format. With this increased usage comes a greater responsibility to ensure the rights and safety of those included in images is safeguarded. As photographic images can be misused through modification or distribution via the internet a number of legal issues must be considered before a decision is made to use such images and how.

1.6 We will inevitably generate images of children, young people and young adults as part of their work to inform, consult and keep records of significant events. Many agencies and organisations use images of people to promote activities and initiatives on behalf of their organisation.

The Aims

- To provide advice and guidance in order to safeguard the students at Spring Hill High School.
- To minimise the risk of misuse of images and to ensure that the students' safety and welfare is not compromised.
- To encourage respect among staff and protect members of staff from Cyberbullying.
- To encourage members of staff to courteous and polite to students, colleagues, parents/guardians and professionals when using electronic devices as a means of communication.
- Protect others' right to privacy and confidentiality

General Policy Statement

2.1 A breach of this policy may result in disciplinary action in accordance with the School's disciplinary procedure. In certain circumstances, e.g. using email to communicate obscene material, or uploading pictures to the Drive that has content that is of an inappropriate nature is a breach of this policy and may be considered to be gross misconduct resulting in dismissal.

Mobile Phones Use

3.1 There has been a growing reliance on the use of personal mobile phones and the temptation for most is to respond to their phone, even if they are engaged with others. It is not acceptable for a member of staff to be supervising students and spending time on their mobile phones. It is extremely important that members of staff maintain high vigilance at all times due to the extreme anxiety and extreme vulnerability of the students in the school. It is impossible to achieve if they are involved in social media messaging while teaching or supervising the students.

3.2 Due to the extreme vulnerability of our students and because we operate on split sites, the school recognises the need for all site leaders to have access to the use of a mobile phone at all times. With this in mind each Deputy has access to a company mobile phone and other leaders are authorised to use their personal mobiles when leading a site to communicate across sites for the safety and welfare of the students.

3.3 All other members of staff must have their personal mobile phones on 'silent' or switched off during times when they are in contact with the students.They may not make or receive calls during teaching time. Use of phones must be limited to non-contact time when no children are present. Phones must be kept out of sight (eg. drawer, handbag, pocket) when staff are with children.
Calls/ texts must be made/ received in private during non-contact time.

3.4 If there are extreme circumstances (eg. acutely sick relative) the member of staff will have made the Headteacher aware of this and can have their phone in case of having to receive an emergency call.

3.5 Phones will never be used to take photographs of students or to store their personal data.

3.6 While on sporting fixtures away from school or on an educational visit for contacting parents in the event of an emergency members of staff are allowed to use personal mobile phones, but the site deputy must be made aware of this upon their return to school.
In the event of an unplanned school closure (ie. snow closure or a heating failure) the school mobile will be used to send each family a text message informing them of the change of circumstances. It is therefore imperative that parents supply school with at least one up-to-date mobile number.

3.7 Staff should never contact students or parents from their personal mobile phone, or give them their mobile number to students or parents. If a member of staff needs to make telephone contact with a parent or student, a school telephone should be used.

3.8 Staff should never send to, or accept from, colleagues or students, text or images that could be viewed as inappropriate.

4.0 Images: Capturing and Using Image

Consent

4.1 Consideration should always be given as to how a particular image is used. If the plan is to take a photograph of people involved in a specific activity or event, there should be no problem in using the image – as long as consent has been granted. Consent is sought for this at the initial interview with the student and the parent/ carer/ social worker has to sign a letter agreeing to the circumscribed use . (see Appendix A) However, if the intention is to use pictures for use in different publications, consideration must be given as to the context in which the image will be appearing.

Reason for capturing images

4.2 Consideration must be given to why a particular activity or event needs to be captured on video or as a photograph. Members of staff are only allowed to capture significant events such as a birthday, Christmas etc. and this must be authorised by the Deputy of the site, Headteacher, Acting RI or Directors.The school may need to keep images for specific pieces of work such as life story work or for wall displays. Members of staff must seek the permission of students before taking photos of them.

4.3 Rules

There are a number of issues staff members need to understand to ensure they are working in a safe way relating to images of students.

- Only use cameras provided by the organisation
- Never take a picture/video of a student on your personal phone
- Never send an image of a student to someone else either within or external to the organisation
- Never upload a picture of a student to Google Drive without authorisation from a site Deputy

- Never upload a picture or videos to Google Drive without the consent of all individuals that are captured in the image.
- Never upload a picture of a young person to a social networking site e.g. YouTube, Facebook, MySpace etc.
- Never share personal images on your mobile phone with students.
- Any member of staff found to be using images of students in their care or who has been in their their in an inappropriate way will face disciplinary action.

Authorised equipment

4.4 Equipment must only be used which is provided or authorised by the organisation, and equipment should always remain in the school. Every school site has an Ipad and cameras that are capable of both capturing still and video images. These will be kept in a safe place in the site office and they are regularly monitored.

Storage and retrieval

4.5 Information from these cameras will be stored in a central location and can be requested by individuals for specific pieces of work. This will be accessed through The School's IT department.. Requests can be made via phone or email, although images will not be emailed.

Unacceptable uses

4.6 Member of staff found taking pictures or capturing images on their personal phones, cameras without authorisation from the Headteacher, Directors, Acting RI or one of the site Deputies will be subjected to disciplinary action.

5.0 Consent

5.1 It is essential that consent is always given by the parent/guardian or carer BEFORE an image is captured. However, members of staff MUST NOT assume that because consent has been given once, it does not need to be obtained again.
5.2 Parents/guardians and carers should be given the opportunity to reconfirm or withdraw their consent for the use of an image.
5.3 Consent will also need to be sought again if it is decided to use an image taken for one purpose in a different context. However, if the purpose remains unchanged it is assumed that consent is indefinite and parents/guardians or carers will be required to contact the headteacher to withdraw consent.

6.0 Email Use

Email is a communication tool and all users must use email in a responsible, effective and lawful manner. Email is provided as part of Spring Hill High School overall provision of ICT facilities for the purpose of teaching, learning, and administration activities. Email use is subject to relevant legislation.

Email Account Access

6.1 Authorised users are issued with an email account by the School's parent company, Thoughts of Others Ltd. This account should be secured by the user with a personal password. An e-mail account may only be used by the person to whom it

is assigned and is not to be shared with anyone for any reason (Other than the reason described below).
A member of staff account and password should be protected accordingly to prevent abuse. Members of staff will be held responsible for any illegal activity that occurs from the use of their account. In some circumstances legitimate access may be allowed to another person's email accounts e.g. For Monitoring and this will be in the event of long term absence due to serious illness or annual leave. Such access to a User's account in these instances must be approved by the head of IT or one of the Directors.

Email Account Closure

6.2 When a member of staff's employment terminates, their email account will be cancelled. The member of staff email account will remain open for a discretionary period, usually one calendar month after a staff member has left.
Staff should ensure that they unsubscribe from any email lists that they have subscribed to and delete any personal emails in their account. If there are any work related emails that need transferring to another user, then these emails should be forwarded on as appropriate.

Compliance with Legislation

6.3 With email as with all other uses of Spring Hill High School and Thoughts of Others Ltd facilities, it is the user's responsibility to make themselves aware of the laws that apply to such use. It should be noted that email messages (deleted or otherwise) may be treated as written evidence in law.
The following are some of the areas of law which apply to the use of email and which could involve liability of users or Spring Hill High School

Intellectual Property

6.4 Anyone who uses email to send or retrieve any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them

Obscenity

6.5 A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.

Defamation

6.6 As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed.

Data Protection

6.7 Processing information, including photographs which contain personal data about individuals, requires the express written consent of those individuals. Any use of personal data beyond that registered with the Information Commissioner will be considered illegal.

Copyright

6.8 The Copyright, Design and Patents Act 1988 are applicable to all types of creations, including text, graphics and sounds by an author or an artist. This will include any which are accessible through Spring Hill High School ICT facilities. Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of their rights.

Discrimination

6.9 Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995, the Human Rights Act 1998 or Employment Equality (Religion or Belief / Sexual Orientation) Regulations 2003 where it involves discrimination on the grounds of sex, sexual orientation, religion, race or disability

Acceptable Use

6.10 Email should be carefully constructed as per other types of correspondence. The users of the email system are responsible for ensuring that they are acting in compliance with legal and acceptable use conditions.
Spring Hill High School will exercise its discretion in judging reasonable bounds within the above standards for acceptability of material transmitted by email.
Spring Hill High School regards the declaration of standards, as described above, to be particularly important. They reflect the values and beliefs of Thoughts of Others Ltd, the parent company of the school.

Personal Use

6.11 Spring Hill High school permits the use of its ICT facilities for email by staff and other authorised users for personal use, subject to the following limitations: a level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided; priority must be given to use of resources for the main purpose for which they are provided. Personal use must not be of a commercial or profit-making nature, or for any other form of personal financial gain. Personal use must not be connected with any use or application that conflicts with an employee's obligations to Thoughts of Others Ltd. as their employer. Personal use must not be connected to any purpose or application that conflicts with Thoughts of Others Ltd's rules, regulations, policies and procedures. Personal use must comply with Thoughts of Others Ltd's policies and regulations.
In relation to the personal use of Spring Hill High School ICT facilities for email, if users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance, in the case of members of staff, of their Line Manager.

Unacceptable Use

6.12 The main purpose for the provision by Spring Hill High School of ICT facilities for email is for use in connection with the teaching, learning, research administrative activities and approved business activities of the school and of Thoughts of Others Ltd. ICT facilities provided by Spring hill High School for email should not be used:

- for personal use, other than as specified in paragraph 5.3.1 above
- for the creation or transmission (other than for properly supervised and lawful information research purposes) of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- for the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- for the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others
- for the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs. Thoughts of Others Ltd is committed to fostering a learning and working environment free of discrimination where everyone is treated with dignity and respect.

Monitoring

6.13 All individuals who hold a specific email account with Spring Hill High school and Thoughts of Others Ltd will be subject to monitoring from the head of IT and Directors.

7. Data protection and E-mail

7.1 As a member of Spring Hill High School every member of staff has certain responsibilities under the General Data Protection Regulations (GDPR), which will form the basis of the Data Protection Act 2018, currently a bill being passed through Parliament. This prescribes a number of further rights and responsibilities in using email as follows:

7.2 Personal data is subject to the Act. Under its terms, personal data includes information that relates to an identified or identifiable individual. So, if it is possible to identify an individual directly from the information you are processing, then that information may be personal data. this would include name, reference or identification number (for example UPN number), location data or online identifier, address, phone number, and email address. If a member of staff include such information in an e-mail or an attachment to an email, you are deemed to be "processing" personal data and must abide by the Act. Personal information includes any expression of opinion.

7.3 Members of staff should be cautious about putting personal information in an email. In particular, they should not collect such information without the individual knowing that they propose to do this. If staff are to send emails containing personal

information to a specified person for a lawful and specified purpose, they shall use encryption software to provide a further step of verification/authentication.

7.4 Members of staff may not disclose or amend such information except in accordance with the purpose for which the information was collected; and they should ensure the information is accurate and up to date.

7.5 Members of staff should not use emails for any purpose that is not permitted by Thoughts of Others Ltd and Spring Hill High School's notification under the Act. Spring Hill High School is permitted to process data for the following purposes: staff, agent and contractor administration; advertising, marketing, public relations; accounts and records; education; research; staff and student support services; other commercial services; Spring Hill High school magazine and journal publication; crime prevention and prosecution of offenders.

7.6 You must not leave electronic devices that contain confidential information logically (e.g. still 'logged-on') or physically insecure (e.g. in an unlocked room) or in such a state that a third party could inspect email or data and gain access to personal information.

7.7 Thoughts of Others Ltd and Spring Hill High school has by law to provide any personal information held about any data subject who requests it under the Act. This includes information on individual PCs in departments and you have a responsibility to comply with any instruction to release such data made by Thoughts of Others Ltd. Emails which contain personal information and are held in live, archive or back-up systems or have been "deleted" from the live systems, but are still capable of recovery, may be deemed accessible by data subjects.

7.8 The regulation also imposes rules on you in retaining personal data. Such data must be kept only for as long as it is needed and for the purpose for which it was collected. Information Services retain deleted emails for three months to allow for accidental loss or any other later requirement by the user for it to be retrieved.

7.9 Members of staff are forbidden from sending emails containing personal information to countries outside the European Economic Area, especially if those countries do not have equivalent levels of protection for personal data.

7.10 Spring Hill High school has taken care to ensure that the information systems and where applicable the supporting infrastructure complies with the relevant legislation and contractual requirements, including:

- The Data Protection Act 1998 and General Data Protection Regulations
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright, Designs and Patents Act 1988
- The Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000

7.11 The IT support team is responsible for ensuring that use of generic access services (e.g. Portal and Internet) within the School complies with the agreed standards and relevant legislation and contractual requirements.

8.0 Internet Use

The Internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of children in embarrassing, inappropriate and even dangerous situations. At Spring Hill High School we recognise the need to ensure responsible use and to protect the safety of children.

Guided educational use

8.1 Significant educational benefits result from curriculum Internet use, including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

8.2 21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become “Internet Wise”. We need to ensure that children and staff are fully aware of the risks, perform risk assessments and implement a policy for Internet use. It is the responsibility of members of staff to ensure that students know how to cope if they come across inappropriate material.

Regulation

8.3 The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within the homes and school must simply be denied, for instance un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

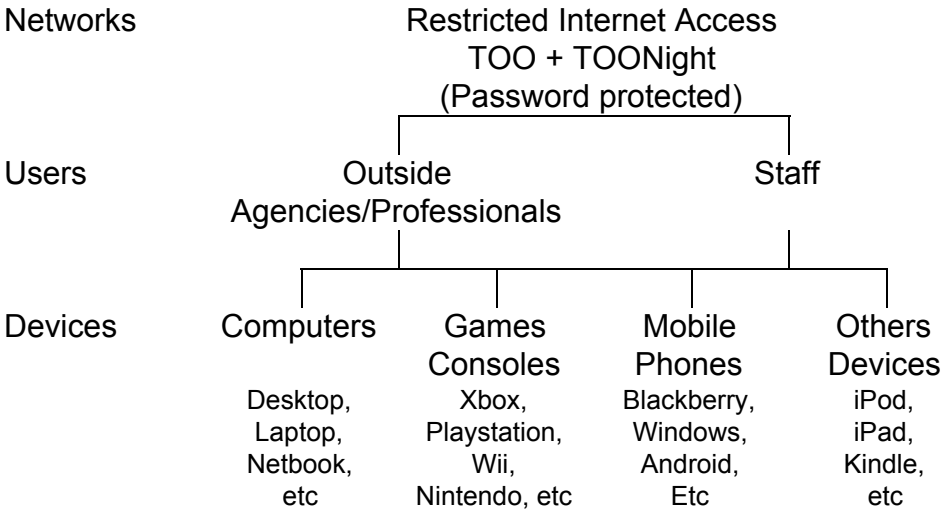
Appropriate strategies

8.4 This policy describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding young people in the appropriate use of the internet.
The most effective strategies have a number of elements that together offer the desired protection for those using the internet. There are a few basic issues that will require staff to ensure:

- They never encourage a student to access inappropriate sites
- Members of staff do not file share with young people
- Staff understand the downloading of material from file sharing sites is not permitted
- Members of staff are aware that when they access one of our internet routers they are subject to the same monitoring procedures as other users on the home.

- Inappropriate use of the internet is a disciplinary offence and will be considered gross misconduct.
- Any member of staff found to be file sharing or uploading any information regarding students or information relating to the organisation will face a disciplinary hearing.

8.5 Internet at Spring Hill High School (this include our Five Homes)



All school sites have restricted wireless internet access ("TOO") for outside agencies and members of staff. Any computers, games consoles, mobile phones or any other internet enabled device using this wired or wireless network are subject to the following limitations.

This internet is only accessible by password and is restricted using OpenDNS Parental Control Filtering Software.

8.7 Blocked Categories

Academic Fraud	Alcohol	Adware
Adult Themes	Chat	Classified
Dating	Drugs	File Storage
Forums/Message Boards	Gambling	German Youth Protection
Hate/Discrimination	Instant Messaging	Lingerie/Bikini
Nudity	P2P/File Sharing	Photo Sharing
Pornography	Proxy/Anonymiser	Sexuality
Tasteless	Tobacco	Video Sharing
Visual Search Engines	Webmail	Phishing Protection

Any computers, games consoles, mobile phones or any other internet enabled device using this wired or wireless network are subject to the following limitations.

All hardware is secured in a locked cabinet and configured at administration level, and can only be accessed, configured or amended by authorised staff.

All Spring Hill High School computers are installed with SpectorsPro's Eblaster software. This enables continual monitoring of all computer usage and produces daily reports of User Activity.

Monitored Categories

- Chat / Instant Messages;
- Online Searches;
- Web Sites Visited;
- Email Activity;
- Files Transferred;
- Keystrokes Typed;
- Program Activity;
- User Activity;
- Keywords Detected;
- Document Tracking;
- Social Media Activity

It is also possible to configure computer specific access or restrictions, these cannot override the homes network restrictions.

8.8 What is Cyber Bullying?

Cyber bullying is the term that's used to describe bullying by one or more people that uses the Internet or mobile phones to threaten, tease or cause deliberate embarrassment to someone. Like any other form of bullying, it can be very distressing for a student or a member of staff to be the subject of cyber bullying.

Although it doesn't involve physical harm, it can be emotionally and mentally harmful, especially when hurtful information is used against you on the Internet or on a mobile phone.

Cyber bullying can involve various different methods, but some of the main ways are:

- Emails – receiving an email that contains upsetting information or is threatening in some way.
- Social networking – profiles that are deliberately set up to mock, tease or embarrass someone else.
- Mobile phones – receiving abusive texts, video messages or photo messages via a mobile phone.
- Chat rooms and instant messaging – receiving abusive messages in chat rooms or via instant messaging.

- Sending viruses – deliberately sending viruses to someone else, that are designed to cause harm to their computer or delete vital information, can be a form of cyber bullying.
- An abuse of personal information – personal details, such as blogs, photos, personal details or photos can be taken and used against someone.

8.9 Unacceptable Use

Some purposes of processing that may constitute unacceptable use include, but are not limited to:

- for the creation or transmission of defamatory material for the creation or transmission of material that includes false claims of a deceptive nature or for so-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms
- for activities that violate the privacy of other users
- for criticising individuals, including copy distribution to other individuals
- for publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author
- for the creation or transmission of anonymous messages, i.e. without clear identification of the sender
- for the creation or transmission of material which brings Thoughts of Others Ltd into disrepute
- for the transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk mail of any kind, to other users, user organisations, or organisations connected to other networks, other than where that material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe
- for the unauthorised transmission to a third party of confidential material concerning the activities of Thoughts of Others Ltd
- for the transmission of material such that this infringes the copyright of another person, including intellectual property rights
- for the unauthorised provision of access to Thoughts of Others Ltd services and facilities by third parties
- for activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users
- for activities that corrupt or destroy other users' data
- for activities that disrupt the work of other user