FOUNDRY COLLEGE

ONLINE SAFETY & INTERNET USE POLICY

Document Control Information

Version	DATE	DESCRIPTION
1	28/08/2015	New policy in line with 360Safety, SWGFL & WBC
2	06/01/2016	Addition of Appendix 1 – Password Policy
3	26/02/2016	Change of Policy Name
4	07/11/2016	Amended in line with KCSIE Sept 2016 doc
5	06/11/2017	Overhaul and update, to improve readability
6	09/11/18	Minor updates, in line with current practice

Reviewed	09/11/2018
Responsibility	Tom Scantlebury
Committee	SLT & T&L
Review Date	November 2019
Signed	Jay Blundell

Background / Rationale

New technologies have become integral to the lives of young people in today's society, both within college and in their lives outside college. However, the use of these new technologies can put young people at risk within and outside Foundry College. Some of the dangers they may face include:

- access to illegal, harmful or inappropriate sharing of personal information
- unauthorised access to, loss of or inappropriate sharing of personal information
- the risk of being subject to grooming
- the sharing or distribution of personal images without an individual's consent or knowledge
- inappropriate communication or contact with others, including strangers
- cyber-bullying
- access to unsuitable film / internet games
- an inability to evaluate the quality, accuracy and relevance of information in the internet
- plagiarism and copyright infringement
- illegal downloading of music, pictures or films
- 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. As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed.

Scope of the Policy

This policy applies to all members of Foundry College, including all individuals who have access to and are users of Foundry ICT systems, both in and out of college premises or time.

The Education and Inspections Act 2006 empowers the Head Teacher, to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the college site and empowers members of staff to impose disciplinary penalties for inappropriate online behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of college. Foundry will deal with such incidents within this policy and associated Relationships / Behaviour and Anti-bullying policies and will, where known, inform parents of incidents of inappropriate internet use that compromise a pupil's online safety, irrespective of whether they take place in or out of college.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the College:

- The Inclusion Manager is the Online Safety Coordinator and is responsible for working with network management provider, TRI Computers.

Foundry College Management Committee

The Foundry College Management Committee has delegated the approval of the Online Safety & Internet Use Policy to the SLT, with overview by the Teaching and Learning Committee.

Headteacher and Senior Leaders

The Headteacher is responsible for ensuring the safety (including online safety) of members of the Foundry family. The day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

The Headteacher and Online Safety Coordinator should be aware of the procedures to be followed in the event of a serious online safety or internet use allegation being made against a member of staff.

Online Safety Coordinator, supported by TRI Computers:

- takes day to day responsibility for all online safety & internet use issues and has a leading role in establishing and reviewing Foundry's Online Safety & Internet Use policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety & internet use incident taking place
- provides and logs training and advice for all staff
- receives reports of online safety & internet use incidents and creates a log of all incidents to inform future online safety & internet use developments
- reports where necessary to SLT and the Teaching and Learning Committee
- liaises with TRI Computers to ensure that the ICT infrastructure is secure and not open to misuse or malicious attack
- ensures that users may only access the Foundry College network through a properly enforced password protected system
- ensures the network is monitored and any attempts at misuse or network outage are reported to the Online Safety Coordinator and Headteacher

Designated Persons for Child Protection / Child Protection Officer

The designated person for child protection should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current relevant policies and practices
- they have read, understood and signed the Foundry College Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problems to the Online Safety Coordinator

- digital communications with pupils, such as email or voice, should be on a professional level only and carried out using official Foundry systems and devices
- online safety is embedded in all aspects of the curriculum and Foundry activities
- pupils understand and follow the Foundry Online Safety & Internet Use Acceptable Use Policy
- pupils have a good understanding of research skills needed to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended college activities
- they are aware of online safety issues related to the use of mobile devices and that they monitor their use
- in lessons where internet is used, pupils should be guided to sites checked as suitable for their use and report any unsuitable sites and materials to the Online Safety Coordinator for blocking
- all pupil laptops are returned to the charging station at the end of lesson or school day
- they take their assigned laptop home at the end of the school day or leave their device in a secure place

Pupils:

- are responsible for using Foundry ICT equipment in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to Foundry equipment
- have an age appropriate understanding of research skills needed to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse and misuse to keep themselves and others safe, and know how to report their worries and observations
- should understand the importance of adopting good online safety practice when using digital technologies
- return laptops to the charging station at the end of lesson or school day

Parents

Some parents may have only a limited understanding of online safety, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's online activities.

Parents do not realise how often or how easily their children come across potentially harmful and inappropriate material on the internet and they are often unsure about what they can do about it and how to go about it. "There is a generational digital divide" (Byron Report).

Foundry College will therefore seek to provide information and awareness to parents through letters, newsletters and the website

Parents will be responsible for

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing Online Safety & Internet Use materials via the Foundry Website

Education of Pupils – The Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of Foundry College's provision. Primary pupils cover this topic through the Jigsaw PSHE programme. Secondary pupils are educated through lessons in "Preparation for Working Life" and

through safeguarding sessions. Children need the help and support of Foundry staff to recognise and avoid online risks and to build their resilience.

Online safety education will be provided in the following ways:

- Online safety will be embedded through the informal curriculum and mentoring conversations wellbeing curriculum
- Pupils will be taught about the importance of critically evaluating the validity of online content.
- Pupils will be helped to understand and respect the need for the Pupil Acceptable Use Policy and encouraged to adopt safe practices when using ICT, the internet and mobile devices both within and outside of Foundry College.

Education & Training: Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online Safety training is part of the planned programme of safeguarding training, mandatory for all staff.
- All new staff will receive online safety training as part of their induction programme, ensuring they understand fully Foundry College Online Safety & Internet Use policies and Acceptable Use Policies.
- The Online Safety Coordinator will receive regular updates by reviewing guidance documents and attending training as required.
- This Online Safety & Internet Use Policy and updates will be presented to and discussed by staff in staff meetings and INSET days, as appropriate.
- The Online Safety Coordinator will provide or facilitate advice, guidance and training to individuals, as required.

Training: Management Committee

Members of the Foundry Management Committee can take part in online safety training and awareness sessions. This may be offered in a number of ways:

- attendance at training provided by relevant organisations
- participation in Foundry College training and information sessions

Technical Responsibilities

Foundry College is responsible for ensuring that the infrastructure and network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. In addition:

- all users will have clearly defined access to Foundry systems. Details of these access rights will be maintained by the Online Safety Coordinator, in discussion with the TRI Computers
- all users will be provided with a username and a password, which they will be required to change immediately so as not to compromise the security of our IT system, by the Online Safety Coordinator. A secure password is required - **Appendix 1**
- all users are responsible for the security of their passwords and should not allow other users to log in using their credentials

- all users are responsible for ensuring their work stations are left “locked” when not in use
- Foundry College maintains and manages the filtering service, in conjunction with Cyberoam and support from Tri Computers
- in the event of a Technician needing to switch off the filtering for any reason, or for any user, this must be agreed by the Headteacher and / or Online Safety Coordinator
- users must report any actual or potential online safety incident to either the Online Safety Coordinator, the Headteacher or Child Protection officer on site
- appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the college systems and data
- temporary access of “guests” onto the Foundry system is allowed at the discretion of the Online Safety Coordinator
- executable files may not be downloaded by users; systems are in place to prevent this
- personal use may be made of laptops and devices out of college, providing the personal information of others held on the device is encrypted and password protected
- removable media, such as memory sticks / CDs / DVDs may be used on Foundry workstations or portable devices, however, they must not be used to install executable files, or to store personal data unless both the data and the removable media device are protected by password and encryption. In practice, this means that most memory sticks will not be suitable for storing personal information relating to others.
- Foundry infrastructure and individual workstations are protected by up to date virus software, Cyberoam
- Personal data may not be sent over the internet, out of the college network unless the subject box is marked [SECURE]

Use of Digital and Video Images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Foundry will inform and educate users about these risks.

Data Protection – See Data Protection Policy

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

At all times, due care will be taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

Personal data will only be accessible using secure password protected devices, and users must ensure that they log-off at the end of any session on any device which has access to restricted data
Data will only be transferred using encryption and secure password protected devices.

Communications

When using communication technologies, the college considers the following as good practice:

- The official college email service can never be deemed totally safe and secure as it is always open to Freedom of Information Requests. Users should be aware that email communications can be monitored. Staff and pupils should therefore only use the college email service for college business.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature to the Online Safety Coordinator or Headteacher. They must not respond to any such communication.
- Any digital communication (email, chat, VLE etc.) used for college business, such as between staff and pupils or parents, other education providers and WBC must be professional in tone and content. These communications may only take place on official college systems. **Personal email addresses, text messaging or social media must not be used for these communications.**
- Pupils should be taught about online safety, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

Appendix 1 - Password Policy

- Passwords must be at least 8 characters long for staff and 6 characters long for pupils and must include 3 of the following:

    - 1 uppercase letter
    - 1 lowercase letter
    - 1 number
    - 1 symbol

- Passwords should avoid following a pattern or being predictable.

- Passwords should not be easily guessable by anyone and therefore should not include :

    - Names of family, friends, relations, pets etc.
    - Addresses or postcodes of same
    - Birthdays
    - Telephone numbers
    - Car registration numbers
    - Unadulterated whole words

Changing Passwords:

- Staff must change their password at least every 90 days. They may not select one of the last 3 passwords used.

- Pupils must be change their password after set up and then at least annually. They may not re-select their last password.

Locked Accounts:

- Staff accounts will be automatically locked out after 5 failed attempts

- Pupil accounts will be automatically locked out after 5 failed attempts

Staff and pupils will need to see the Online Safety Coordinator or contact Tri Computers to unlock their account