SUTTON COLDFIELD GRAMMAR SCHOOL FOR GIRLS

E- SAFETY AND SECURITY POLICY

DATE: June 2018
REVISION DATE: June 2019

Background / rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to: General Data Protection Regulation (GDPR), Freedom of Information Act 2000 and the current edition of 'Keeping Children Safe in Education'.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- access to illegal, harmful or inappropriate images or other content
- unauthorised access to/ loss of/ sharing of personal information
- the risk of being subject to grooming by those with whom they make contact on the internet
- the risk to propaganda which may result in radicalisation
- the sharing/ distribution of personal images without an individual's consent or knowledge
- inappropriate communication/ contact with others, including strangers
- cyber-bullying
- access to unsuitable video/ internet games
- an inability to evaluate the quality, accuracy and relevance of information on the internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- 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 and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. Behaviour for Learning, Anti-Bullying, Safeguarding and Child Protection policies and the Staff Code of Conduct). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We will provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks whilst students are within school using school equipment. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/ carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Student Body
- Student and parent questionnaires
- Student focus group discussions
- School website and newsletters

Scope of this policy

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/ carers, visitors, community users) who have access to and are users of school ICT systems, both in and

out of school.
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.
Students may also be disciplined at any time when their behaviour:

- Could have repercussions for the orderly running of the school or
- Poses a threat to another student or member of the public, or
- Could adversely affect the reputation of the school.

(DFE guidance for Headteachers and Governors Jan. 2016)
This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will apply appropriate school sanctions where actions outside school are known and damage the school reputation or cause distress to other students or staff.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT, PSHE and other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial /pastoral activities
- Students are taught in all lessons to be critically aware of the materials they access on-line and guided to validate the accuracy of information
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- E-safety prefects lead an e-safety team and deliver assemblies to their peers.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Digital Technologies Systems Manager or Technician can temporarily remove those sites from the filtered list for the period of study.

Student Evaluation of Internet and Online Content
The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email, text message or social media requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Students are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

Education – parents / carers
Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, the website, the weekly parents' email bulletin and the VLE
- Parents' evenings

- Signposting useful sources of information such as Think U Know - How to Guides, Child Exploitation and Online Protection (CEOP): http://www.ceop.gov.uk/reporting_abuse.html. and NSPCC Net Aware - Guides to Social Media

Education and Training – Staff

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

A planned programme of formal e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the performance management process and training will be provided accordingly

All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

Training – Governors

Governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any subcommittee involved in ICT, e-safety, health and safety and child protection. This may be offered in a number of ways:

- Completing online e safety training
- Participation in school training / information sessions for staff or parents

Information Systems Security Maintenance

- It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and students. ICT security is a complex issue which cannot be dealt with adequately within this document. Relevant identified firewalls, filter software and virus protection for the whole network is installed and is current.

Local Area Network (LAN) security issues include:

- Workstations are secured against user mistakes and deliberate actions.
- Servers are located securely and physical access is restricted.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA encryption.
- The security of the school information systems and users is reviewed regularly by the Digital Technologies Systems Manager.
- Virus protection is updated regularly.
- Unapproved software will not be allowed.
- Files held on the school's network are regularly checked.
- The Digital Technologies Systems Manager reviews system capacity regularly.
- The use of user logins and passwords to access the school network is enforced.

Email Management

Email is an essential means of communication for both staff and students. In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, students and other professionals for any official school business. This is important for confidentiality, GDPR compliance, security and also to safeguard members of staff from allegations.

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a designated member of staff if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.

- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- The forwarding of chain messages is not permitted.
- Staff will follow the procedures in the 'IT and Personal/Sensitive Data Acceptable Use Statement and Agreement' when sending emails.

Management of Published Content

Publication of any information online should always be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or students' personal information will not be published.
- Email addresses will be published carefully online, to avoid them being harvested for spam
- The school website complies with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever, even after we have deleted such files as part of our Data Retention Policy and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital /video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Written permission from parents or carers will be obtained before images and/or videos of students are used (covered in the 'Images and Videos Parental Consent Form' signed by parents/carers of existing students in May 2018, and for new students as they join the school). Staff will check whether parents/carers have provided consent for the specific purpose: e.g. displays within school, on the weekly parents' bulletin, on the School website, on the School social media sites, in the local press and/or School publicity material. Students' work can only be published with the permission of the student and parents or carers.
- Care should be taken when taking digital /video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Management of Social Networking and Social Media

Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- The school will control access to social media and social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM, (Instant messaging) and email addresses, full names of friends/family, specific interests and clubs etc.

- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to only approve and invite known friends on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage and /or inappropriate use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour is outlined in the school Acceptable Use Policy and in the staff Code of Conduct.

Internet Filtering

It is important to recognise that filtering is not 100% effective.
Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school has a clear procedure for reporting breaches of filtering. All members of the school community, (all staff and all students), will be aware of this procedure (contact the Digital Technologies Systems Manager or Technician).
- If staff or students discover unsuitable sites, the URL will be reported to the Digital Technologies Systems Manager who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

School Response to Incidents of Concern

E-Safety Complaints

E-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about students and in developing trust so that issues are reported.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school will determine the level of response necessary for the offence disclosed.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school behaviour for learning policy where appropriate.
- The school will inform parents/carers of any incidents of concern, as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the e-Safety officer and where necessary escalate the concern to the Multi Agency Safeguarding Team, Police or other agencies.

Cyber Bullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" - DCSF 2007

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour for learning.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and other agencies, if necessary.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying and behaviour for learning policies or the acceptable use policy.
- Parent/carers of students will be informed.

Use of the Virtual Learning Environment

- Students/staff will be advised about acceptable conduct and use when using the VLEs, this includes sites such as Show my Homework, Office 365 and other web based learning portals used by the school.
- Only members of the current students, Y6 students using the transition site, parent/carers and staff community will have access to the VLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled.

Use of Mobile Phones and Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players etc. can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features. However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their use can render students or staff subject to cyberbullying.
- Internet access on phones and personal devices can allow students to bypass school security settings and filtering.
- They can undermine classroom discipline.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of students or staff.

Due to the widespread use of personal devices it is essential that the school takes steps to ensure mobile phones and devices are used responsibly at school and it is essential that student and staff use of mobile phones does not impede teaching, learning and good order in classrooms.

- The use of mobile phones, smart watches and other personal devices for accessing the internet, social media, text messages and calls by students is not permitted in the classroom, or form rooms. Mobile phones and other devices may only be used in the dining room and the hall before 8.40 am. Phones must be switched off from 8.40 am to 3.40 pm and must not be switched on again until students have left the school site. Mobile devices, including phones, must never be used at any time in the school car park. Sixth form students may be permitted to use their own devices as part of a planned lesson and only when given specific instructions and permission by staff.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour for learning policy.

- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- If a student needs to contact their parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Link2ICT E-safety Policy. http://www.link2ict.org/school-improvement/courses-by-category/esafety
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Any filtering issues should be reported immediately to the Digital Technologies Systems Manager or Technician.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Digital Technologies Systems Manager, and/or the designated safeguarding lead.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. Guest speakers are provided with a generic, limited account on which to logon and use the school system. Trainee teachers are provided with unique staff accounts in order to access network resources.
- An agreed policy is in place regarding the downloading of executable files by users. Users are not advised to download executable files unless under the advice or authorisation of ICT staff.
- The school infrastructure and individual workstations are protected by up to date recognised Anti-virus software.
- Personal and/or sensitive data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Staff are asked to be mindful of intellectual property and must not copy such material onto memory sticks for example, in particular where this would infringe copyright.

School trips and off-site activities

Where school trips and other off-site activities take place which may lead to the use of ICT or raise e-safety and security issues; the trip provider will be provided with a copy of this policy and asked to take all reasonable steps to comply with the policy as far as is practical.

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

- logs of reported incidents

- internal monitoring data for network activity
- surveys / questionnaires/focus groups consisting of:
    - students
    - parents/ carers
    - staff

INITIAL EQUALITY IMPACT ASSESSMENT FORM

Name of policy/activity/project:
E-Safety Policy

Is this a new or an existing policy/activity/project?
Existing policy

Scope/timescales for project or activity (including review date):
To be reviewed in March 2019

Policy/project lead and Author of Equality Impact Assessment:
Mrs L. Long

Outline of main aims of this activity/policy/project:
To provide guidelines for all members of the school community about the school's expectations and actions with regard to E-Safety

Who will benefit/be affected by this policy/activity?
Staff, students and community users of Sutton Coldfield Grammar School for Girls

If an existing policy/activity, do you have any data of use by or impact on different groups which may raise concerns over an equality impact?
No

Does the activity have the potential to impact differently on groups due to a protected characteristic (eg race/ethnicity, gender, transgender, disability, religion & belief, age, sexual orientation, maternity/paternity) for:
No

(a) Students and members of the community? (Eg The Governing Body, students, contractors, visitors, hirers of the premises, agency staff, suppliers etc). Which groups are likely to be affected?
The provisions of the policy are equally applicable to all.

(b) Employees?
The provisions of the policy are equally applicable to all.

Does this activity make a positive contribution to the School's general or specific duties under the Equality Act 2010? If yes, please detail.
Yes – the Policy applies to all students and staff equally

Having reviewed the potential impact of the policy/activity listed above, **I believe a full impact assessment is required / NOT required** (delete as applicable with justification below)

Full impact assessment is not required

Justification: The policy is of equal benefit to all students, regardless of gender, race, religion, sexual orientation etc.

Name : Mrs L. Long…… Date : ……June 2018……..