GREENSIDE FILM FACTORY

E-Safety Policy

September 2019

The Governing Body of Greenside School adopted this policy on 1st Sept ‘17

GREENSIDE
Use of digital and video images

At Greenside:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins Greenside;
- Digital images /video of students are stored in a private Greenside Google Drive folders and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials / DVDs;
- Staff, students and parents sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- The school blocks/filters internet access and specifically to social networking sites or newsgroups unless there is a specific approved educational purpose. Anything inappropriate that should get through the filter is logged and blocked by Greenside's ICT provider.
- Students are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger students as part of their ICT scheme of work;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Our school Social Media sites are managed by a member of the Leadership Team and posts are checked before going live. All posts are related to Greenside learning experiences or events. Any person trying to 'follow' Greenside is checked before acceptance.
- Comply to all relevant GDPR regulations and follow TEF guidelines for GDPR.

Website:

- The Head of School takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: Deputy Heads, Business Leader and Administration Assistant.
- The Greenside web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. admin@schooladress. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning platform:

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools platform will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved and closed systems, such as the Learning Platform;
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' Learning Platform for such communications.

CCTV:

- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Managing the Internet Safely
Technical and Infrastructure approaches

Greenside:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;.
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and students cannot download executable files;
- Uses individual, audited log-ins for all users;
- Uses DfE, LA, RM or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Only uses the LGfL / NEN service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level.
- Uses security time-outs on Internet access where practicable / useful;
- Provides staff with an email account for their professional use, *TEF Gmail* and makes clear personal email should be through a separate account;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;

- Has additional local network auditing software installed;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Uses Google Drive to store all documentation in line with TEF / GDPR guidelines.

Policy and procedures

Greenside:

- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures students only publish within the appropriately secure school's learning environment, such as Google Classroom.
- Requires staff to preview websites before use [where not previously viewed or cached] or uses QR codes to direct students and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids
- Is vigilant when conducting 'raw' image search with students e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the ICT Leader. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;
- Requires students to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Ensures parents/ carers provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for students, staff and parents/ carers
- Provides E-safety advice for students, staff and parents/ carers;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police, TEF, LA as appropriate.

- Fosters a ‘No Blame’ environment that encourages students to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches students and informs staff what to do if they find inappropriate web material i.e. close ipad and report the URL to the teacher or System Manager.
- Ensures students and staff know what to do if there is a cyber-bullying incident;
- Ensures all students know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / TEF London / national guidance. Students are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older students] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand ‘Netiquette’ behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older students] to understand why and how some people will ‘groom’ young people for sexual reasons;
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming / gambling;
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents/ carers/ carers/ carers, including:
    - Information leaflets; in school newsletters; on the school website;
    - demonstrations, practical sessions held at school;
    - distribution of ‘think u know’ materials for parents/ carer or similar supportive websites;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents/ carer

Appendix 1

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places students in an embarrassing or potentially dangerous situation.

Surfing the Web Aimless surfing should never be allowed. It is good practice to teach students to use the Internet in response to an articulated need – e.g. a question arising from work in class. Students should be able to answer the question "Why are we using the Internet?"Search engines can be difficult to use effectively and students can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger students 'searching the Internet'.

Students do not need a thousand Websites on weather. A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites / bookmarks are a useful way to present this choice to students. QR codes are also a good way to direct students to specific sites that have been checked.

Teachers' web site selections for various topics can be put onto a topic page on the Learning Platform so students can access out of school, from home etc. Some schools put links on their school website, although there may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing. Therefore, sites should always be previewed and checked, and work for students is best located on the closed Learning Platform.

Search Engines

Some common Internet search options are high risk, for example 'Google' image search. Some LAs and Councils block this. Others keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution and follow the school's guidelines. LGfL guidance is available on the e-safety site. Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to students and staff.

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping students consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as Google Classroom.

Blogs / Google Classroom

We sometimes use Blogs as a method of online publishing, perhaps creating class blogs, or to creatively support a specific school project. A 'safe' blogging environment is likely to be part of a school's Learning Platform or within LGfL /LA provided 'tools'. All blogging activity is sent to class teachers for moderation before appearing on the site. This includes any external comments. Google Classroom is a private and secured digital learning environment where only students within TEF can gain access and only when invited directly by a member of staff. This can be used to share documents or learning outcomes.

Webcams and Video Conferencing

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. LGfL has a number of nature cams showing life inside bird boxes for example and a plethora of weather cams across London providing detailed real-time weather data. Webcams can also be used across London for streaming video as part of a video conferencing project.

Video conferencing provides a ‘real audience’ for presentations and access to places and professionals – bringing them into the classroom. For large group work high quality video conferencing hardware equipment is required to be plugged into the network. LGfL, and the other national regional grids for learning, have made an agreement with JVCS (the Janet Video conferencing Service) to host calls. All conferences are therefore timed, closed and safe. This is a service that is included in LGfL 2. Advice can be found here
http://www.lgfl.net/SERVICES/CURRICULUM/Pages/WeatherStations.aspx
http://www.lgfl.net/learningresources/VideoConferencing/Pages/Home.aspx

Students can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with students.

The highest risks lie with streaming webcams [one-to-one chat / video] that students use or access outside of the school environment. Students need to be aware of the dangers.

Social Networking Sites

These are a popular aspect of the web for young people. Sites such as Facebook, My Space, Habbo Hotel, Bebo, Piczo, and YouTube allow users to share and post web sites, videos, podcasts etc. It is important for students to understand that these sites are public spaces for both students and adults. They are environments that should be used with caution. Users, both students and staff, need to know how to keep their personal information private and set-up and use these environments safely. [See Education programme]

At Greenside we block such sites. However, students need to be taught safe behaviour as they may well be able to readily access them outside of school. There are educational, monitored services that schools can purchase such as GridClub SuperClubs. Additionally, the LGfL Learning Platform provides a safe environment for students to share resources, store files in an ePortfolio, and communicate with others through ‘closed’ discussions, etc.

Podcasts

Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables students to create their own radio broadcast and post this onto the web. Students should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area.
http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx

Chatrooms

Many sites allow for ‘real-time’ online chat. Again, students should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Students should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chat rooms such as www.teenchat.com, www.habbohotel.co.uk, www.penguinchat.com

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be immediately referred to the Police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.