Greenvale School
E-Safety Policy and Protocol

Signed: November 2018
Next Review date: November 2019

The E-Safety Leader is also the Designated Safeguarding Lead: Felicia Hughes

- The E-Safety Protocol has been written by Greenvale staff, building on LSCB and government guidance. It has been agreed by staff and school leaders and approved by governors
- The E-Safety Protocol and its implementation are reviewed annually.

The school understands the benefits and the risks to young people of using the Internet and this document outlines the procedures we have put in place to ensure that the children in our care become safer, more discerning users of the Internet and related technologies wherever this is possible.
Adults, as well as young people, can find themselves vulnerable to malicious use of the Internet both in their personal and professional lives. The E-Safety Protocol highlights the importance of training and guidance in good practice in safer use of the Internet for staff. The protocol also recognises that there are other safety issues associated with using technologies, such as over-exposure to LCD screens, privacy etc.
The Internet and associated technology is a rapidly evolving environment where new opportunities and risks appear daily. As far as possible Greenvale teaches young people how to manage existing risks and understand the dynamic nature of technologies, so that they are able deal confidently with challenges in the future, whatever they might be.

Rationale & Links with Other Policies/Curriculum Areas

- Child Protection & Safeguarding Policy
- Keeping Children Safe in Education Sept 2016 (statutory guidance)
- PSHE curriculum
- Computing Curriculum
- Data Protection policy (with particular reference to email guidelines)
- Acceptable Use Agreement
- Home School Agreement
- Anti-Bullying Policy and Procedure
- Staff Code of Conduct

UNICEF Rights' Respecting Article 17: Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

1. Teaching and learning

As we move towards a more digital curriculum, we acknowledge and will actively promote the use of 'real-world' technologies as an aid to learning.

1.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. Schools have a responsibility to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and students.

1.2 Internet use will enhance learning

- The school's Internet access will be designed expressly for student use and will include filtering appropriate to the age of students (Appendix 1)

- Wherever possible, students will be taught the differences between acceptable and unacceptable Internet use and given clear objectives for Internet use.

- The school is vigilant in their supervision of students' use at all times, as far as is reasonable, and common-sense strategies are applied where older students have more flexible access.

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Teachers will update and check websites before accessing with the children to ensure that the content is appropriate. The curriculum is planned in context for internet use to match students' ability and skills.

- To promote learners' independence and sense of personal responsibility, students who are able to, sign an E-Safety/ acceptable use statement which is fully explained and used as part of the teaching programme. Appendix 2

- Parents provide consent for students to use the Internet, as well as other IT technologies, as part of the E-Safety acceptable use agreement form at time of their child's entry to school.

- Wherever possible 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, parent workshops and the curriculum.

- A record is kept of any cyber-bullying or inappropriate behaviour in-line with the school's behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours.

- The school ensures the Designated Safeguarding Lead Professionals have appropriate training in E-Safety practice.

- The school provides advice and information on reporting offensive materials, abuse/ bullying etc. and makes this available for students, staff and parents/carers.

- E-Safety advice for students, staff and parents is provided.

- The school 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.

- The school ensures that staff and student (as far as is possible) understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include; risks in pop-ups; buying on-line; on-line gaming / gambling, in app purchases.

- The school ensures staff know how to send or receive sensitive and personal data and understand the requirement to protect data through password protection or encryption.

- The school makes training on E-Safety available to staff as part of the cycle of Safeguarding training.

- The school runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; practical sessions; in school newsletters; on the school web site;
  - distribution of 'think u know' for parents materials https://www.thinkuknow.co.uk/teachers/resources/
  - suggestions for safe Internet use at home;
  - provision of information about support sites for parents, e.g. CEOP and UK Safer Internet Centre, ChildNet (Appendix 3)

1.3 Students will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and students complies with copyright law.
- Students, wherever possible, are taught a range of skills and behaviours appropriate to their age, experience, and needs - such as:
    - to STOP and THINK before they CLICK
    - to discriminate between what might be true or false from Internet information
    - to skim and scan information;
    - to be aware, wherever possible, that websites involve bias and are often self-seeking in nature. To know how to narrow down or refine a search;
    - For students who are able - 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;
    - For students who are able, to have strategies for dealing with receipt of inappropriate materials;
    - to understand online purchasing e.g. apps and within app purchases
    - For students who are able, to understand why and how some people will 'groom' others with inappropriate or illegal motives

2. Managing Internet Access

2.1 Information system security

- The school's IT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.

2.2 E-mail

- Students may only use approved school e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters or similar 'spam' is not permitted.

2.3 Published content and the school web site

- The contact details on the Web site are the school address, e-mail and telephone number. Staff, student or governors' personal contact information will not be published.
- The Executive will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing student's images and work

There is a separate Photographs, Digital and Video Images Policy for the School.

- Photographs that include students will not reference their full name. Digital images /video of students stored in a teacher's documents or shared images folder on the network are

deleted when the student leaved the school at the end of Y14 or if leaving sooner, when they are taken off roll.

- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school.
- Students are not identified by their full name in online photographic materials in the credits of any published school produced video materials / DVDs.
- Parental agreement is obtained, through the consent form signed at point of admission, before students images are published on the school's website or other publications e.g. local newspapers.
- Student's work can only be published externally with the permission of the student and parents/carers.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/devices and personal equipment for taking pictures of students (Appendix 5)
- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school
- Wherever possible, students are taught about how images can be manipulated and possible implications of this, in E-Safety education and the PSHE curriculum.

2.5 Social networking and personal publishing

- The school blocks/filters access to social networking sites or newsgroups unless there is a specific, approved educational purpose.
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. Wherever possible they are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that networking sites have Terms and Conditions, such as minimum age which must be observed.
- Newsgroups will be blocked unless a specific use is approved.
- Students are advised never to give out personal details of any kind that may identify them or their location, or that of family or friends.
- Students and parents are advised that the use of some social network spaces, for example Facebook, Instagram, Twitter, SnapChat, etc. outside school might be inappropriate for students, that they can be vulnerable when using these spaces and that some of these sites have minimum age requirements.
- Wherever possible, students are taught that they should not post images or videos of others without their permission on websites or apps. They are taught 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, including the use of geolocation permission settings. They are taught the need to keep their data secure and what to do if they are subject to bullying or abuse. Appendix 7

2.6 Preventing Radicalisation

- Protecting children from the risk of radicalisation should be seen as part of school's wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation it is possible to intervene to prevent vulnerable people being radicalised.
- The internet and the use of social media in particular has become a major factor in the radicalisation of young people.

- As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include making a referral to the MASH or Prevent/Channel Team.

- Schools and colleges must ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

  Keeping Children Safe in Education (2016)

2.7 Managing filtering

- The school will work with relevant providers to ensure systems which protect students are regularly reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the SLT. Concerns are escalated to the technical service provider as necessary.
- The school will immediately refer any material we suspect is illegal to the appropriate authorities e.g. Police, and the local authority.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. These will be tested regularly by the technical service provider.

2.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

2.9 Protecting personal data

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

3. Policy Decisions

3.1 Authorising Internet access

- All staff and students (or parents/carers on their behalf) have signed an acceptable use agreement form that requires that they report any concerns.
- The school reserves the right to withdraw Internet access from a student or member of staff in the event of misuse or infringement of policy.

3.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LBL can accept liability for the material accessed, or any consequences of Internet access.
- The school will review ICT policy, protocols and provision regularly to establish whether the E-Safety policy is adequate and that its implementation is effective.

3.3 Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a member of SLT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection/safeguarding nature must be dealt with in accordance with schools' safeguarding procedures.
- Students and parents are able to access the Complaints Procedure on the school website or request a hard copy document from the school office.

- On rare occasions the procedures for handling potentially illegal issues will involve the school contacting the police

3.4 Community use of the Internet

- The school will liaise with local organisations that use school facilities to establish a common approach to E-safety.

4. Communications Policy

4.1 Introducing the E-Safety protocol to students

- E-Safety rules are displayed in all classrooms and other work areas and are discussed with the students on a regular basis, including during planned curriculum provision
- Students are informed that network and Internet use will be monitored.

4.2 Staff and the E-Safety

- The E-Safety Protocol is distributed to all staff and is included in the cycle of annual safeguarding training sessions.
- Internet usage is able to be monitored and can be traced to the individual user. Discretion and professional conduct is essential.

4.3 Enlisting parents' support

- Parents/carers' attention will be drawn to the school E-Safety Protocol in a variety of ways including: newsletters, the school brochure and on the school Web site.

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. Wherever possible, students will be taught how to respond if such a situation arises.

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.
- Search engines can be difficult to use effectively and students can experience overload and failure if the set topic is too open-ended. It may not always be appropriate for students to be 'searching the Internet'.
- Students do not need a thousand Web sites 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/ability group and fit for purpose. Favourites / bookmarks or hyperlinks within a document are a useful way to present this choice to students.

Search Engines

- Internet search engines are managed through the LGfL provider, this service ensures that appropriate filters and restrictions are put in place to reduce the risk of students accessing inappropriate material.
- Copyright rules must be considered by staff when using material from the Internet and when students download material e.g. Images. 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 children consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as the London MLE.

- Blogs: A School may want to use them 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'.
- These are a popular aspect of the web for young people. Numerous sites allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces for both children 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.
- Most schools will 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 children to create their own radio broadcast and post this onto the web. Children 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

Sanctions and infringements

- The E-Safety/Acceptable Use policy is made available and explained to staff /Governors, students and parents, and acceptance/agreement forms are completed appropriate to their age and role. Failure to comply with the Acceptable Use Agreement may result in sanctions applied from the school's student Behaviour Policy or staff Code of Conduct Policy.

- Incidents relating to Child Protection/Safeguarding will result in referrals via the MASH to external agencies such as, the police, LADO and Children's Social Care.

Signed

Dated

Appendix 2

E-Safety Form for Students'

Think before you click

I will only use the internet and email with an adult

I will only click on icons and links when I know they are safe

I will only send friendly and polite messages

If I see something I don't like on a screen, I will always tell and adult

My Name:

My Signature:

Appendix 3

Parents E-Safety Agreement Form

Parent / guardian name: _____ _____

Student name(s): _____

As the parent or legal guardian of the above student(s), I grant permission for my daughter or son to have access to use the Internet, London Grid for Learning (LGfL) e-mail and other ICT facilities at school.

I know that where appropriate my daughter or son has signed an e-safety agreement form and been shown the rules for responsible ICT use.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to students.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: Date: _____/_____/____

Use of digital images - photography and video:

I also agree to the school using photographs of my child or including them in video material, as described in the school's Photographs, Digital and Video Images Policy. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school and for no other purpose.

Parent / guardian signature:_____ Date: _____/_____/_____

Appendix 4

Staff Acceptable Use Agreement

This agreement covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head Teacher and Governing Body.
- I will not reveal any personal password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business which is currently staff mail unless approved by the Head Teacher or School Business Manager.
- I will only use the approved school email, school MLE or other school approved communication systems with students or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / e safety co-ordinator.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission.
- If applicable, I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role, and will not in any way bring the school or colleagues into disrepute by inappropriate postings on social networking sites.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure that any equipment taken out of school on loan other than during school visits will be my responsibility and should loss/damage occur liability will be covered by personal insurances.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the school's information

management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage and e-mails can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies & protocols.
- I agree to abide by all the points above.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature _____ Date _____

Full Name _____ (printed)

Job Title _____

School _____

Authorised Signature (Deputy Head Teacher/School Business Manager

I approve this user to be set-up.

Signature _____ Date _____

Full Name _____ (printed)