GENEVA ENGLISH SCHOOL

E-SAFETY POLICY

INTRODUCTION

It is the duty of Geneva English School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smartphones and tablets.

This policy, supported by the Acceptable Use of IT Policies, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection
- Health and Safety;
- Behaviour and Discipline;

- Anti-Bullying;
- Acceptable Use of ICT;
- Data Protection;
- Remote Working and Use of Personal Devices;
- Taking, Storing and Using Images of Children.

Whilst exciting and beneficial both in the context of education and elsewhere, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At GES, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties, as well as their thoughts and ideas.

SCOPE OF THE POLICY

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policies cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards and digital video equipment); as well as all devices owned by pupils, staff, or visitors and brought onto school premises including personal laptops, tablets, and smartphones.

ROLES AND RESPONSIBILITIES

Governors

The Governing Body of the School is responsible for the approval of this policy and for reviewing its effectiveness. The Governing Body will review this policy at least annually. The Governor with responsibility for Safeguarding and Child Protection will liaise with the e-Safety Officer in relation to all e-Safety matters and will report back to meetings of the Board of Governors.

Head and Senior Leadership Team

The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the e-Safety Officer, Ronan McStravick. In particular, the role of the Head and the Senior Leadership Team is to ensure that:

- staff, and in particular the e-Safety Officer, are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the School.

E-Safety Officer

The School's e-Safety Officer is responsible to the Head for the day to day issues relating to e-safety. The e-Safety Officer has responsibility for ensuring this policy is upheld by all members of the school community and works with all staff and pupils to achieve this. He/she will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

The e-Safety Officer will also be responsible for the e-safety education for all GES pupils, deal with incidents in liaison with the DSLs and will meet regularly with the Safeguarding and Child Protection Governor to discuss current issues, review incidents and discuss any changes to procedures and practice.

Network Manager

The School uses an external company (ART Computer) to manage and maintain the safety of its technical infrastructure. They advise on the security of the School's hardware system and should report any concerns to the e-Safety Officer.

Teaching and Support Staff

All staff are required to sign the Acceptable Use of IT Policy for Staff and Governors before accessing the School's systems. As with all issues of safety at GES, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis. Staff should report any suspected misuse or problem to the e-Safety Officer and help students understand and follow the e-Safety and Acceptable Use of IT policies.

Designated Safeguarding Leads

The School's Designated Safeguarding Leads are trained in e-safety issues and made aware of the potential for serious child protection and safeguarding issues.

Pupils

Pupils are responsible for using the school IT systems in accordance with the Pupil Acceptable Use of IT Policy, and for letting staff know if they see IT systems being misused.

Parents and carers

GES believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School via the e-Safety Officer.

Parents and carers are responsible for endorsing the School's Pupil Acceptable Use of IT Policy and signing the Parent Acceptable Use of IT Policy.

EDUCATION AND TRAINING

Staff awareness and training

New staff receive information on the GES e-Safety and Acceptable Use Policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All non-teaching staff receive information about e-safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's e-Safety Officer or Designated Safeguarding Lead.

Pupils: e-safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about e-safety within a range of curriculum areas and Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHCE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHCE or Computing lessons, pupils are taught about their e-safety responsibilities and to look after their own online safety. From Year 7, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Designated Safeguarding Leads, the e-Safety Officer, or to any member of staff at the School.

From Year 7, pupils are also taught about relevant laws applicable to using the Internet, such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through classroom discussions and activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-Bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Designated Safeguarding Leads, the School Counsellor, or the e-Safety Officer as well as parents, peers and other school staff for advice or help if they experience problems when using the Internet and related technologies.

Parents

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The e-Safety Officer therefore sends a regular e-safety bulletin in the newsletter and provides the same information on the School's website. The e-Safety Officer also organises at least one parents' forum per year to discuss and answer questions about e-Safety. In this way we aim to help parents minimise the potential dangers of IT to their children.

PUPILS' USE OF SCHOOL AND PERSONAL DEVICES

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they must be handed in to Reception at the start of the day and collected as they leave school (Primary) or should be kept switched off and out of sight in their lockers all day (Secondary). These devices will remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

No personal devices belonging to pupils are to be used during lessons at school, whether for school work or personal use.

School mobile technologies available for pupil use (including laptops, tablets, cameras, etc.) are stored in locked charging facilities at GES Primary and the IT room at GES Secondary. Access is available via the class teachers. Members of staff should ensure all devices are returned to the charging facilities at the end of each lesson.

The School recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Head to agree how the School can appropriately support such use. The Head, Deputy Head or Assistant Head will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

DIGITAL COMMUNICATION

Staff

Staff must immediately report to the e-Safety Officer the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the e-Safety Officer.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- Bring Geneva English School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Any digital communication between staff and pupils or parents must be professional in tone and content.

Pupils

All pupils are issued with their own personal school e-mail addresses for use on our network and by remote access. Access is via a personal login on Google, which is password protected. This official email service may be regarded as safe and secure, and must be used for all relevant school work. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork or research purposes, pupils should contact the e-Safety Officer for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the e-safety officer or other member of staff. The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the e-safety officer or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour and Discipline Policies. Pupils should be aware that all internet usage via the School's systems and its wifi network is monitored.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for schoolwork or research purposes, pupils should contact the e-Safety Officer for assistance.

DATA STORAGE AND PROCESSING

The School takes compliance with Data Protection legislation very seriously. Please refer to the Data Protection Policy and Privacy Notices for further details. Staff and pupils are expected to save all data relating to their work to their school Google Drive account or to the School's central server. Staff devices should be encrypted if any data or passwords are stored on them. The School expects all removable media (USB memory sticks, CDs, portable drives) to be encrypted before being used. Staff may only take information off-site when authorised to do so, and only when it is necessary and required in order to fulfil their role.

No personal data of staff or pupils should be stored on personal memory sticks or personal online storage platforms, but instead stored on the school's server or school Google Drive. Please refer to the School's Remote Working and Use of Personal Devices Policy for more information. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the e-Safety Officer.

SAFE USE OF DIGITAL IMAGES

For the School's policy on the safe use of digital images, please see the Taking, Storing and Using Images of Children Policy

MISUSE

GES will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the School's policies and procedures (in particular the Safeguarding and Child Protection Policy). In line with our Anti-

Bullying Policy, the School will impose sanctions on any pupil who misuses technology to bully, harass or abuse another pupil.

COMPLAINTS

As with all issues of safety at GES, if a member of staff, a pupil or a parent has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Officer in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate.

Incidents of or concerns around e-safety at school should be recorded using an Incident Report form and reported to the school's e-Safety Officer. Instances involving possible harm to children must be reported to the Designated Safeguarding Lead.

Anyone suspecting that:

- access has been attempted to any website containing child abuse images
- access has been attempted to any website containing obscene material
- access has been attempted to any website containing criminally racist material
- access has been attempted to any website which contains statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity
- any such materials are to be found on any electronic device, whether owned by the School or not
- there has been any incident by electronic means of 'grooming' behaviour

must report all allegations, complaints, concerns or suspicions directly to the Head or, in his absence, to the Chair of Governors, unless that person is the subject of the concern; those about the Head should be reported to the Chair of Governors (or in her absence, the Vice Chair).

Action from this point will be dictated by the Safeguarding and Child Protection Policy and Procedures.

Concerns, suspicions or allegations of other IT related illegal activity (such as fraud, copyright theft or unlicensed use of software) by a member of staff should also be reported according to the reporting hierarchy outlined above. Such concerns will be managed in accordance with the School's Whistleblowing Code.

IT INVESTIGATIONS

Where directed to so so by the Head, Chair or Vice Chair of Governors, DSL or Deputy DSL, or by an external agency such as the Police, the e-Safety Officer will undertake investigative actions. These may include:

- Examination of materials stored on the School's storage networks, taking copies of any items associated with the incident in question;
- Remote examination of school desktop and laptop computers and the gathering of relevant evidence, including the copying of materials or the taking of screen captures;

- Examination of the contents of school e-mail mailboxes, including sent and deleted items, and the extraction of messages and materials relevant to the incident in question;
- The requiring of staff to return school-owned digital devices to the Head of Computing for investigation.

These investigations will be carried out by the e-Safety Officer under the supervision of the Head (or in his absence, the Deputy Head). Unsuitable materials will be copied and may then, under the direction of an appropriate authority, be deleted from storage, mailboxes or computers.

At the end of the investigation, a report on all materials and references found, detailing the processes followed, will be passed to the Head, unless that person is the subject of the concern.

Investigations surrounding the Head, including examination of the contents of school e-mail inboxes, will be carried out by the e-Safety Officer under the supervision of the Chair of Governors (or in her absence, the Vice Chairman).

Ronan McStravick, e-Safety Officer and Head of Computing & Digital Strategy
Created: September 2018
Review: July 2019