Date: September 2017
Review date: September 2018
Responsibility: HAE/KP

FIDES et OPERA

Bromley High School

E - SAFETY POLICY

Girls' Day School Trust

Introduction and scope of the Policy

This policy seeks to formalise the management of E-safety risks, incidents, and education within the school. It should be read in conjunction with the school *Safeguarding and Child Protection Policy*, the GDST *Safeguarding Procedures* (which incorporate the staff *Code of Conduct*), and the *Anti-Bullying Policy*. These detail the steps that should be taken in any safeguarding issue whether it is mediated by technology or not.

While many of the risks around E-safety will be familiar, modern technologies have created a landscape of challenges and dangers that are still constantly changing. The continued development of systems and devices means that school leaders will need to be proactive and pragmatic in dealing with problems and threats as they emerge.

This E-safety Policy applies to all members of the school community including staff, students/pupils, volunteers, parents/carers, and visitors. It applies to the whole school, including the Early Years Foundation Stage.

The nature of E-safety and GDST School Provision

Internet access is a feature of everyday life both in and out of school. Pupils and staff may use a number of networks and a range of devices in a single day and each may have different levels of access and capability.

Nevertheless, Bromley High School and the GDST believe that schools should be safe environments for learning. We judge the safeguarding of pupils both inside and outside school to be of the highest priority and therefore we adhere to the following principles:

- The highest standards of technological protection are included as part of school networks.
- Pupils are taught about E-safety in all its aspects as part of the curriculum, and E-safeguarding is seen as a responsibility of *all* staff.
- The school regards E-safety education as an important preparation for life.
- The school recognises that pupil and family information is sensitive and private. Data protection is regarded as a high priority.

1. Systems and Procedures

School Procedures and responsibilities

The school has identified a member of staff to co-ordinate E-safety, Mrs Sabine Lawton, who will work closely with the Designated Safeguarding Leads. However E-safety is seen as a whole-school issue, and different members of staff will have responsibilities as listed below.

Headmistress	• Has overall responsibility for E-safety provision. • Has overall responsibility for data and data security (SIRO). • Ensures that the school uses the GDST filtered Internet Service. • Ensures that staff receive suitable training to carry out their E-safety roles and to train other colleagues, as relevant. • Is aware of the procedures to be followed in the event of a serious E-safety incident. • Receives regular monitoring reports from the E-safety Co-ordinator / Officer. • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures (e.g. network manager). • Oversees the staff Acceptable Use arrangements and takes appropriate action over staff who breach them.

Designated Safeguarding Leads	• Takes day to day responsibility for E-safety issues and assumes a leading role in establishing and reviewing the school E-safety policies / documents. • Facilitates training and advice for all staff. • Is the main point of contact for pupils, staff, volunteers and parents who have E-safety concerns. • Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. • Ensures that the E-safety incident log is kept up to date. • Communicates with SLT to discuss current issues and filtering. • Liaises with relevant agencies. • Ensures that staff and pupils are regularly updated in E-safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): o sharing of personal data o access to illegal/inappropriate materials o inappropriate on-line contact with adults/strangers o cyber-bullying o sexting
Computing Curriculum Leaders and E-safety advisors	• Oversees the delivery of the E-safety element of the Computing curriculum. • Liaises regularly with the Designated Safeguarding Leads over E-safety. • Promotes an awareness and commitment to e-safeguarding throughout the school community (pupils and parents). • Ensures that E-safety education is embedded across the curriculum • Ensures that the Acceptable Use agreement is posted at key points around the school • Keeps the E-safety pages for parents and pupils up to date and relevant • Liaises with relevant E-safety organisations. • Contributes to helping the DSL ensure that staff and pupils are regularly updated in E-safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): o sharing of personal data o access to illegal/inappropriate materials o inappropriate on-line contact with adults/strangers o cyber-bullying o sexting.
Network Manager/ E safety co-ordinator	• Reports any E-safety related issues that arise to the Designated Safeguarding Leads • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Ensures that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • Ensures the security of the school ICT system. • Ensures the physical security of the school ICT system • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices (eg use of encrypted USB sticks, Safend, MBAM etc) • Ensures that the policy on web-filtering is applied and updated on a regular basis.

	• Ensures that GDST IT Department is informed of issues relating to filtering applied by the Trust. • Keeps up to date with the school's E-safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant. • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keeps up-to-date documentation of the school's E-security and technical procedures. • Keeps an up to date record of those granted access to school system. • Liaises with school IT technical staff and relevant E-safety agencies. • Ensures that the school is compliant with all statutory requirements surrounding the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. • Ensures that GDST guidance and policies on the handling of information are implemented. (Guidance is available on ORACLE). • Produces and distributes regular safeguarding reports on internet activity
Teachers	• Embed E-safety issues in all aspects of the curriculum and other school activities. • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content (eg copyright laws)
All staff	• Read, understand and help promote the school's E-safety policies and guidance. • Are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use and implement current school policies with regard to these devices. • Report any suspected misuse or problem to the E-safety coordinator. • Maintain an awareness of current E-safety issues and guidance, eg through CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff AUP.
External groups	• Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Filtering and monitoring

Currently, all schools within the GDST are centrally provided with their data connections via a dedicated network. All incoming data are initially screened via an application that provides real-time filtering and protects both networks and users from internet threats. It prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to educational material from (for example) YouTube. The policy determining filtering is managed centrally, with different levels being applied depending on age group.

See filtering categories in Appendix A

The filtering system produces a weekly report which identifies situations where students have tried to access sites which may give rise to concern. Monitoring can also be undertaken on a needs basis. For example, reports can be generated about the types of sites being accessed by users of the system and the number of times they have been requested

There is also a centrally managed process for scanning email messages between staff and students for inappropriate language and behaviour. If there is an issue the HR department at Trust Office will be alerted and the matter is taken up with the school. Email traffic between pupils is not scanned as a matter of course, but if concerns about contacts between pupils are raised, then a record of messages can be retrieved by GDST IT.

The DSL keeps a log of all E-safety incidents in the school and shares this on a regular basis with the senior leadership team and school network manager. The E-Safety Co-ordinator monitors the implementation of the E-safety Policy and ensures that its provisions are being implemented.

Acceptable Use Agreements and authorising internet access

Before using any school IT resource all staff members are required to read and sign an Acceptable Use Agreement (AUA) as part of their contract of employment. Staff have a dedicated log-on which requires them to use a strong password for access to the system. The first time they log on, an automatic on-screen message reminds them about their responsibilities under the AUA and requires them to acknowledge this. Their response is then logged.

Differing versions of this agreement may be used to match the personal and professional roles of staff members. A copy of the agreement will be given to staff members for their reference. The AUA details how school equipment and connections may be used.

A separate register of when pupils were given (and agreed to abide by) the provisions of the agreement is kept for future reference with the pupil's records.

The school will keep a record of all staff and pupils who are granted Internet access through the individual usernames granted. The record will be kept up-to-date. (This will take account of changes such as a member of staff who has left the school or a pupil whose access has been withdrawn.)

Visitors to the school can be given access to the Internet by connecting to Visitor wireless. The filtering and monitoring systems apply as above. Access for visitors is provided under the general terms and conditions of the GDST, which prohibit the sending or receiving of materials which "are offensive, abusive, defamatory, obscene, or menacing" or which are illegal. The visitor signs a disclaimer which outlines restrictions and expectations of use.

Staff use of Equipment and the Internet

The equipment provided for staff is primarily intended to support the teaching and learning of pupils. However, it is unreasonable to deny staff access to the internet for legitimate personal use (for example to contact a son's or daughter's school). Nevertheless, discretion and the highest professional standards are expected of staff using school equipment.

Expectations are set out in detail in the *Acceptable Use Agreement* and in the *Social Media Policy,* but include:

- Keeping a proper professional distance e. g. not “friending” pupils on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or e-mails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents.

Misuse of school systems
Because the staff *Acceptable Use Agreement* is part of the contract of employment, misuse is a disciplinary matter.

Pupil misuse (for example the sending of bullying messages to another pupil) may result in the withdrawal of facilities or further sanctions in line with the school's disciplinary policy.

Abuse of the systems by visitors will result in the immediate withdrawal of access and possible further action depending on the nature of the misuse.

2. E-safety, Pupils, and Safeguarding

Teaching E-safety in School
The school curriculum includes lessons and activities in E-safety for all pupils.
The intention is to develop pupils' awareness, resilience, and skills in the wider electronic world.
Pupils will explore issues such as:
- **Persuasion and reliability** (internet scams, phishing, unreliable information, radicalisation and extremism, etc.);
- **Personal information and safety** (sexting, social network information, personal images, etc.);
- **Sexual exploitation** (grooming, "offender not present" activities, etc.);
- **Online bullying** (text abuse, “trolling”, etc.).

The activities are differentiated with regard to age.

The curriculum is varied and may comprise:
- staff-led skills sessions (e.g. How to configure *Facebook* privacy settings)
- whole-school assemblies led by older pupils, and other examples of peer mentoring
- discussion groups
- ‘Safer Internet Day’ activities
- formal lessons.

The teaching covers not only what the problems are, but how to deal with and avoid them. Wherever possible, we engage older pupils to share their experiences and advise others about personal safety and responsibility online.

These activities and lessons form part of the Computing/IT and PSHE schemes of work.

There is a dedicated area on Firefly for E-safety with links to presentations and useful sites.

The E-safety Co-ordinator keeps up to date on emerging trends and advises on the focus of the curriculum appropriately.

Staff training and updates
- All staff will have E-safety training included as part of their safeguarding induction to the school.
- All staff receive regular training in safeguarding pupils. E-safety is included as part of this.
- E-safety incidents and concerns are a standing item at staff briefings.
- Training on the implementation and use of Impero for monitoring pupil online activity

Guidance to pupils on using e-mail and other messaging systems

- When using the school system, pupils may only use approved email accounts.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

As part of the *Acceptable Use Agreement*, pupils undertake never to send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students are reminded that the sending of abusive messages is illegal.

Particular concerns:

Inappropriate material appearing on school computers

- Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting. They are encouraged to talk to their teacher. The teacher should report the incident to the E-safety Co-ordinator or DSL who will log the problem and liaise with the network manager to adjust filtering settings.

Abusive messages on school computers

- Pupils who receive abusive messages over school systems will be supported, and advised not to delete messages. The DSL will be informed and an investigation begun initially with the help of the Network Manager.

Pupil reporting outside school

- Pupils are taught that if something worries them, or if they think a situation is getting out of hand, that as well as talking to a teacher they can share this with their parents, and consider using the online **Report CEOP** button to make a report and ask for help.

Mobile data

- Whilst access to the internet using the GDST network will be subject to filtering and monitoring, the school is aware that many children will have unlimited and unrestricted access to the internet, for instance via 3G and 4G personal devices, both whilst in school and outside school. However, the AUA the pupils sign and the school's e-safety education cover the responsible use of IT in any situation, whether using the school's networks or not.

Reporting of E-safety concerns

The school takes reports concerning E-safety very seriously. The action taken depends on the nature of the concern raised.

All incidents that come to the attention of school staff should be notified to the E-safety Co-ordinator.

The E-safety Co-ordinator will ensure that pupils, parents, volunteers, and staff understand that they can contact them with concerns at any time.

Any incident that raises wider safeguarding questions will also be communicated to the Designated Safeguarding Lead(s) and action under the *Safeguarding Policy* and *Procedures* will be considered.

School Website

Advice, guidance, and links are available through the school's website for parents and pupils. This advice includes details of how to report a problem to the school, and which members of staff have responsibility for resolving a problem or taking issues further. The school also has an anonymous reporting system (Confide) which will enable anyone with a concern to share it with the school easily and directly.

3. Risk Management – Everyday E-safety

Assessing risks

The school will take all reasonable precautions to ensure that users abide by the acceptable use rules and access only appropriate material.

The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use rules which are published for their protection.

Due to the international scale and linked nature of internet content, it is also not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

The school cannot accept liability for material accessed, or any consequences of internet access.

Staff using IT equipment will mainly be covered by the provisions of the *Display Screen Equipment (DSE, Health and Safety) Regulations* 1992. Guidance, definitions, and requirements can be found on the Health and Safety section of the GDST staff intranet.

The use of DSE by pupils is not covered by the *Display Screen Equipment Regulations*. However, it is good practice to apply the requirements of the legislation to their workstations thus helping them to develop safe working practices. In particular it is recommended that adjustable seats are provided at pupil workstations and they should be given guidance on appropriate work positions and routines.

If pupils are issued with laptops, tablets, etc. then a risk assessment must be completed and guidance on how to use them given safely. A template risk assessment and pupil advice sheet can be found on the GDST staff intranet Health and Safety Section.

Use of mobile phones and cameras

In order to prevent allegations of inappropriate activities, including against EYFS staff, staff must not store images of pupils (taken in a school capacity) on any personal device.

Any images taken on personal devices must be downloaded to school or GDST systems as soon as reasonably possible and the personal copy permanently removed (please refer to the school's policy on Cameras, recording devices and mobile phones.) Staff must be careful to avoid taking any photos of pupils that could be construed as inappropriate, and any photos that may inadvertently be seen as inappropriate should be destroyed.

Publishing staff & pupil information and photographs

- **The school website**

The contact details on the website are the school address, email and telephone number. Staff contact details include a school email address. Pupils' personal information will not be published.
The Headmistress has overall editorial responsibility and ensures that content is accurate and appropriate.

- **Publishing pupils' images and work on the web**

o **Open / public sites**

Public sites could potentially be used to gather information and the locations of pupils. Written permission to publish photographs and work on websites have been obtained as part of the contract signed by parents. However, unless there is need to identify a pupil (eg. to celebrate a prize) the following guidelines should be observed:

1. Pupils' full names will not normally be used on the website or blog, particularly in association with photographs.
2. Photographs published on the website or elsewhere, which include pupils, will be selected carefully. Care will be taken when taking digital/video images that pupils are appropriately dressed.

o **Closed/ Secure sites**

Pupils' images, video, and work can be made available to parents on secure areas of the web as long as the following measures are adhered to:

1. The parents/carer are issued with a secure log-on to view the information on their pupils.
2. Parents should be made aware that their child's images may be included in group work viewable by other parents/carers.

Using websites with pupils

Pupils are often directed to internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing digital world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- All sites are filtered via the "Fortinet" system to minimise the risk of inappropriate material being accessed.
- If pupils are asked to make online accounts for access to materials, the minimum of identifiable personal information will be disclosed and only school emails will be used.
- The school will be as open as possible about the sites and software it uses, and it welcomes queries from parents who wish to raise concerns or understand more about the way that IT contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions which do not apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risks will be assessed. It should be understood that potential problems or harm may not emerge until after the adoption of a technology.

The senior leadership of the school (including the E-safety Co-ordinator) will reassess the suitability of technology and systems over time and check that they remain suitable, secure, and effective.

Handling E-safety complaints

Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the procedures of the school and according to the nature of the complaint.

Any complaint about staff misuse must be referred to the Headmistress.

For impartiality, investigations into IT misuse by school staff will be carried out by the GDST's IT Security & Compliance Manager.

Complaints of a child protection nature are dealt with in accordance with statutory child protection procedures.

Pupils and parents are informed of the school's complaints procedure.

Using non-School Equipment –"Bring Your Own Device"
Under some circumstances, teachers and pupils are now able to use their own equipment in school and connect to the available network. This is normally called "bring your own device" (BYOD).

Whether staff member or pupil, it is made clear to the user that the rules and expectations surrounding online behaviour remain in force regardless of the ownership of the equipment being used. Please refer to the school's Mobile Device Policy.

4. Communicating the Policy

Introducing the E-safety policy to children

- Versions of the E-safety/Acceptable Use rules are discussed with pupils as needed. The aim is to keep the policy familiar and fresh for pupils rather than treated as something which is only referred to at odd times.
- Pupils are made aware that network and internet use is monitored.

Staff and the E-safety policy

- All staff will have the importance of the E-safety Policy explained to them.
- They signed a copy of the Staff Acceptable Use agreement as part of the contract of employment.
- Staff should be aware that internet traffic and email can be monitored and traced to the individual user. Because of this, discretion and professional conduct are essential.

Communicating E-safety information to parents

- The school website gives information on E-safety and how the school can help.
- E-safety advice will be included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.
- The school holds E-safety events to brief parents about E-safety developments and policies; possibly as part of events such as 'Safer Internet Day'.
- Wider information events for parents will have E-safety items included in the programme.