CITY OF LONDON SCHOOL FOR GIRLS
IT & ESAFETY ANNEX

ROLES & RESPONSIBILITIES

This section outlines the roles and responsibilities for eSafety of individuals and groups within the school.

GOVERNORS

Governors are responsible for the approval of the eSafety policy and for reviewing the effectiveness of the policy. Governors will also need to adhere to having a professional online presence in line with the school's guidance.

HEAD TEACHER & SENIOR LEADERSHIP TEAM (SLT)

The Head Teacher is responsible for ensuring:

- The safety (including eSafety) of all members of the school community, although the day to day responsibility for eSafety may be delegated to the eSafety Coordinator.
- Adequate training is provided.
- Effective monitoring systems are set up.
- That relevant procedure in the event of an eSafety allegation are known and understood.
- Establishing and reviewing the school eSafety policies and documents (in conjunction with eSafety co-ordinator).
- The Deputy Head (Pastoral) will be responsible for overseeing any issues regarding eSafety and work closely with the eSafety Coordinator in creating the appropriate safeguards for pupils.
- The school's Designated Child Protection Officers should be trained in eSafety issues and be aware of the potential for serious child protection issues to arise through the use of IT.
- Work with external organisations as described in statutory guidance Working Together to Safeguard Children 2015.

ESAFETY COORDINATOR

The eSafety Coordinator takes day to day responsibility for eSafety issues and has a leading role in:

- Liaising with staff, ICT Technical staff and SLT on all issues related to eSafety as well as reporting any safeguarding issues to the Designated Safeguarding Leaders.
- Working closely with the Deputy Head Pastoral on how to promote eSafety within the school as well as how to deal with issues that may arise.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.

- Providing training and advice for staff.
- Monitoring the school activity using the Securas software and logging and acting upon incidents that they might come across.
- Receiving reports of eSafety incidents and creates a log of incidents to inform future eSafety developments.
- Co-ordinating and reviewing eSafety education programme in school.
- Providing a platform to inform parents on eSafety and how to ensure that they are putting the right safeguards in place at home regarding their internet services, communication with their children as well as how to manage the use of iPad's supplied by the school.

DIRECTOR OF IT

The Director of IT is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets eSafety technical requirements.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Keeps up to date with eSafety technical information.
- The use of the school's ICT infrastructure (network, remote access, e-mail, etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the eSafety Coordinator and/or SLT for investigation/action/sanction.
- Ensure that Safe User Agreements are up to date and signed for school devices as well as the iPad Programme, liaising with the eLearning Coordinator to ensure that pupils are adhering to the agreements and that there are no abuses of the programme.
- To ensure that the pupils are safe from terrorist and extremist material when accessing the internet in school by establishing appropriate levels of filtering.

TEACHING & SUPPORT STAFF

In addition to elements covered in the Staff Acceptable Usage Policy, all teaching and support staff are responsible for ensuring that:

- Adhere to The Teachers' Standard 2012 safeguarding children's wellbeing and sense of trust.
- They have an up to date awareness of eSafety matters and of the current school eSafety policy and practices.
- They have read, understood and signed the school Staff Acceptable Usage Policy.
- ESafety issues are embedded in all aspects of the curriculum and other school activities.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- They report any incidents to the eSafety Coordinator, DSL, or Deputy Head (Pastoral) and are aware of possible signs where children are at risk or vulnerable.
- Be aware of the City of London CSE Operating protocol from May 2015 and keep abreast of Government material such as Keeping Children Safe in Education.

STUDENTS

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety policy also covers their actions out of school, if related to their membership of the school.
- Students understand and follow the school's eSafety and acceptable usage policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

PARENTS/CARERS

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policies.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.
- Reading advice provided by the school to ensure that they are able to protect their children at home and create a working dialogue with their children about eSafety issues.

Written: September 2015
Approved by Board of Governors: 22nd October 2015
To be reviewed by: October 2018