Local Procedure Title	**E-Safety**
Service	**Roehampton Gate School**
ACS Policy number and title	**ACS 38 E-Safety**
Local Procedure template reference	**ACS LP 38**
Local Procedure date	19-09-2025
Local Procedure review date	19-09-2026
Local Procedure Author(s)	Lucia Apicella
Local Procedure Ratification	Checked and Approved by:

1. Introduction`

All staff at Roehampton Gate School understand the importance of emerging technologies for Children's educational and personal development and seeks to support children and young people in making use of these in our work; however, we also recognise that safeguards need to be in place to ensure young people are kept safe at all times.
The purpose of this procedure is to:

- Set out the key principles expected from all staff at RGS, with respect to the use of ICT- Based technologies
- Safeguard and further protect our young people
- Assist staff working with children/YP to work safety and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with other safeguarding policies
- Ensure that all members of staff are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal actions will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

2. Main Risks

The main areas of risk for Roehampton Gate School, can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identify theft (including 'frape' (hacking Facebook profiles) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputations
- health and well-being (amount of time spent online (Internet or gaming))

- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

This policy applies to all members of staff, students/pupils, volunteers, parents / carers & visitors who have access to and are users of Aspris ICT systems.

3. Key Responsibilities

Headteacher:

- To take overall responsibility for e-safety provision
- To take overall responsibility for data and data security (SIRO)
- To ensure the sites use an approved, filtered Internet Service, which complies with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- To be aware of procedures to be followed in the event of a serious e-safety incident.
- To receive regular monitoring reports from the safeguarding DSL's in relation to E-safety
- To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures

Designated Safeguarding Leads:

- To take day to day responsibility for e-safety issues at their sites and has a leading role in establishing and reviewing the site e-safety policies / documents
- To promote an awareness and commitment to e-safeguarding throughout the service
- To ensure that e-safety education is embedded across the curriculum
- To liaise with school ICT technical staff
- To communicate regularly with SLT / regional safeguarding leads to discuss current issues, review incident logs and filtering / change control logs
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- To ensure that an e-safety incident log is kept up to date
- To facilitate training and advice for all staff
- To liaise with the Local Authority and relevant agencies
- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying and use of social media

Teachers:

- To embed e-safety issues in all aspects of the curriculum and other school activities
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff:

- To read, understand and help promote the sites e-safety policies and guidance
- To read, understand, sign and adhere to the sites Acceptable Use Agreement / Policy
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- To report any suspected misuse or problem to the DSL's
- To maintain an awareness of current e-safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with young people should be on a professional level and only through company based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils:

- Read, understand, sign and adhere to the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand service agreement on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
- To help the school in the creation / review of e-safety policies

Parents/carers:

- To consult with the school if they have any concerns about their children's use of technology
- To communicate with school in regards to the technologies purchased for young people

External groups:

- Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

4. Handling complaints:

Roehampton Gate School will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by teacher/ Head Teacher/ DSL
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system.
- referral to LA / Police.

Our DDSL's act as first point of contact for any complaint. Any complaint about staff misuse is referred to the safeguarding lead.

Complaints related to child protection are dealt with in accordance with safeguarding policy.

5. Review and Monitoring

The e-safety procedure is referenced from within other local procedures & policies: Safeguarding
The e-safety procedure will be reviewed annually or when any significant changes occur with regard to the technologies in use within the service
The e-safety procedure has been written by the service DDSL and is current and appropriate for its intended audience and purpose.
There is widespread ownership of the procedure and it has been agreed by the SLT and by approved stakeholders. All amendments to the e-safeguarding procedure will be discussed in detail with all members of senior staff.

6. Expected conduct

In Roehampton Gate School, all users:

- Are responsible for using the ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to computer systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- 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 e-safety practice when using digital technologies out of work and realise that the service's E-Safety procedure covers their actions out of work, if related to their workplace or employer
- will be expected to know and understand company policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand company policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the service e-safety procedure and using the company ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the service

- should know and understand what the 'rules of appropriate use' are and what consequences result from misuse

7. Incident Management

In Roehampton Gate School:

- there is strict monitoring and application of the e-safety procedure and a differentiated and appropriate range of consequences, though the attitudes and behaviour of users are generally positive and there is rarely need to apply these.
- all site staff and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the sites escalation processes.
- support is actively sought from other agencies as needed (e.g. CEOP, the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the service . The records are reviewed/audited and reported to the sites SLT/the LA / LSCB
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or young person's receives online communication that we consider is particularly disturbing or breaks the law
-

8. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

Roehampton Gate School

- Has the educational filtered secure broadband connectivity through the Aspris Network
- Uses the Net Sweeper 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 are logged and only available to staff with the approved 'web filtering management' status
- Ensures network healthy through use of Sophos anti-virus software. and network set-up so staff and pupils cannot download executable files.
- Uses DfE, LA or Aspris approved systems such as S2S, Voltage, 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;
- Individually risk assess access to certain websites for specific purposes;
- Works in partnership with Aspris to ensure any concerns about the system are communicated so that systems remain robust and protects users
- Is vigilant in its supervision of use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Informs all users that Internet use is monitored

- Informs staff and students that that they must report any failure of the filtering systems directly to staff. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or IT Helpdesk as necessary
- 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
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate server access
- We provide pupils with an individual network log-in username.
- All pupils have their own unique username and password which gives them access to the Internet
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through approved systems
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security

Password policy

- RGS makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff have their own unique username and private passwords to access company systems. Staff are responsible for keeping their password private
- We require staff to change their passwords regularly

E-mail

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous.

Social networking

ALL staff are instructed not to run social network spaces for student use on a personal basis or to open their own spaces to their students.

RGS's staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or company staff
- They do not engage in online discussion on personal matters relating to members of the workplace
- Personal opinions should not be attributed to the *co*
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

9. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into RGS are entirely at the staff member, student's & parents' or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into site.
- Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the manager. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny, and the manager is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The school reserves the right to search the content of any mobile or handheld devices on the premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone in an agreed location, Staff Room, Deputy head or Assistant head office.
- Mobile phones and personally owned devices may not be used in any way during lessons or formal school time.

Students' use of personal devices

- Mobile phones are not permitted on site; they are to be handed into reception and locked away in secure individual phone locker.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of

mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children/young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a work phone where contact with parents or carers is required.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the site policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

10. Digital images and video

In Roehampton Gate School

- We gain parental / carer permission for use of digital photographs or video involving their child/YP as part of the site agreement form when their child joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published company produced video materials / DVDs;
- Staff sign the sites Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long term use
- Children/young people are advised to be very careful about placing any personal photos on any 'social' online network space. As part of PSHE, they are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- As part of PSHE, children/young people 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, 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

Contents Checklist (Local Services may add additional items – this is a core list)			
Local responsibilities		Risk assessments	
Contact plans		Access to email	
Correspondence		Access to social media	
Access to telephones		Children and young people's own communication devices	
Record keeping		'Local Rules' for safe and sensible communications and social media use	
Monitoring arrangements			

Local Procedure Review History:

Date Reviewed	Reviewer	Summary of revisions