London South East Academies Trust

E-Safety Policy

Responsible post holder	Trust Board
Approved by / on	July 2018
Reviewed	July 2019
Reviewed	July 2020
Reviewed	August 2021

This policy is part of the Trust's Statutory Safeguarding Policy/ Procedures. Any issues and concerns with online safety must follow the Trust's safeguarding and child protection processes.

Contents

6. Equipment and Digital Content
    - Personal mobile phones and devices
    - Storage, Synching and Access
    - Digital images and video
7. Education at Home

Appendices (separate documents):

A1 Exemplar Acceptable Use Agreement (Visitor and Contractors)

A2: Exemplar Acceptable Use Agreements (Pupils – adapted for phase)

A3: Exemplar Acceptable Use Agreement including photo/video permission (Parents)

A4: Data security

A5: **Guidance: What we do if?**

A6: LGFL Filtering Provider Checklist

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the **London South East Academies Trust** with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist Academy staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice including remote learning.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole Trust community.
- Have clear structures to deal with online abuse including peer to peer sexual harassment such as online bullying [noting that these need to be cross referenced with other Trust policies].
- Ensure that all members of the Trust community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our Trust community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Being groomed (sexual exploitation, radicalisation etc.)
- Being bullied online
- Being victim of social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying) and sexual harassment
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)

- Sexting – Youth Produced Sexual Imagery
- Copyright (little care or consideration for intellectual property and ownership)

Commerce

- Online gambling
- Inappropriate advertising
- Phishing
- Financial scams

Scope

This policy applies to all members of **London South East Academies Trust** including staff (supply staff incluced), pupils, volunteers, parents/carers, visitors, community users who have access to and are users of **London South East Academies Trust** IT systems

Roles and responsibilities

Role	Key Responsibilities
Headteacher/ Heads of School	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Partners guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To ensure there is a high quality remote learning package in place for all learners when required which is in line with safeguarding procedures for the school and Trust for both pupils and staff • Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information • To ensure the schools use appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident

Role	Key Responsibilities
	• To ensure Trustees are regularly updated on the nature and effectiveness of the schools' arrangements for online safety • To ensure school websites include relevant information.
Designated Safeguarding Lead	• Lead role in establishing and reviewing the schools' online safety policy/documents • Promote an awareness and commitment to online safety throughout the School community • Ensure that online safety education is embedded within the curriculum for the School • Liaise with school technical staff where appropriate • To communicate regularly with SLT, HT/ HoS and the designated safeguarding Trustee to discuss current issues, review incident logs and filtering isuues • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • "Liaise with the local authority and work with other agencies in line with Working together to safeguard children" • Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns. • To ensure that online safety incidents are logged as a safeguarding incident • Work with the HT, Heads of School, DPO and trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns. • Ensure the 2021 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying • Facilitate training and advice for all staff: o all staff must read KCSIE Part 1 and all those working with children Annex A

Role	Key Responsibilities
	○ it would also be advisable for all staff to be aware of Annex C (online safety) ○ cascade knowledge of risks and opportunities throughout the organisation
Trustees	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the E Safety Policy and review the effectiveness of the policy • To support the schools in encouraging parents and the wider community to become engaged in online safety activities • Work with the DPO, DSL and HT/ HoS to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information • Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in schools
ICT Curriculum Leader	As listed in the 'all staff' section, plus: • Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum and using Teaching online safety in school as guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
Network Manager/technician	• To report online safety related issues that come to their attention, to the Designated E Safety Lead, SLT and HT/ HoS • To manage the schools' computer systems, ensuring - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices

Role	Key Responsibilities
	• That they keep up to date with the school's e safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of schools technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to Heads of School/ HT. • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the schools following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all relevant sections). • 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 • To monitor online behaviour in class and report any concerns to appropriate SLT • Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself • Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils) • Take a zero-tolerance approach to bullying and sexual harassment (your DSL will disseminate relevant information from on this but also in Trust Policy format) • Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment

Role	Key Responsibilities
	and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know. • Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. • Ensure all Remote Learning tasks are appropriate, safe and of high quality
PSHE / R(S)E /Health Education Lead/s	• Due to R(S)E now being statutory: • Embedding mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds." • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE
Subject / aspect leaders	• As listed in the 'Teachers section, plus: • Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike using 'Teaching online safety in school' as guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf • Consider how the UKCCIS framework Education for a Connected World can be applied in your context • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Quality assure all Remote Learning tasks to ensure appropriate, safe and of high quality
Data Protection Officer (DPO)	• Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education September 2021' and 'Data

Role	Key Responsibilities
	protection: a toolkit for schools' (September 2018), especially this quote from the latter document: • GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding • The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)' • Work with the DSL, HoS, HT and Trustees to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. • Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
All staff, supply staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates at least annually. The AUP is signed by new staff on induction • To report any suspected misuse or problem to the Designated Safeguarding Lead • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the schools. This will include leaving IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse including sexual abuse and harassment, 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school during remote learning as well as socially and realise that the schools' online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To report any concerns regarding any type of abuse or harassment that their child or any other may be experiencing • To consult with the schools if they have any concerns about their children's use of technology • To support the schools in promoting online safety including the pupils' use of the Internet and the schools' use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within schools • To support the schools in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

This policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school's website
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school

Handling Incidents:

- The schools will take all reasonable precautions to ensure online safety

- Staff and pupils are given information about infringements in use and possible sanctions
- Heads of School/ Headteacher will act as first point of contact for any incident
- Any suspected online risk or infringement is reported to Designated Safeguarding Lead on that day
- Any concern about staff misuse is always referred directly to the Headteacher/ Head of School, unless the concern is about the Headteacher/ Head of School in which case the compliant is referred to the Deputy CEO (Academies) and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident (YPSI):

Please see separate policy Youth Produced Sexual Imagery Policy

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding, Anti-Bullying policy, PSHE, Peer on Peer Abuse/ Harassment, ICT policy).

- The e safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the schools. It has been reviewed due to changes in Keeping Children Safe in Education September 2020.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Trustees. All amendments to the Trust e safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

The following subjects have the clearest online safety links:

- PSHE
- Health Education, Relationship Education in primaries and in secondaries, Relationships and Sex Education
- Computing

The Trust will ensure the schools will:

- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.
- Ensure there is a high quality remote learning package in place for all learners when required which is in line with safeguarding procedures for the school and Trust for both pupils and staff

- Use ‘Teaching online safety in school’ (June 2019) and ‘Education for a Connected World’ (June 2020) as key guidance documents to pursue a whole school approach including:
    i) Creating a culture that incorporates the principles of online safety across all elements of school life
    ii) Proactively engaging staff, pupils and parent/ carers
    iii) Reviewing and maintaining the online safety principles
    iv) Embedding the online safety principles
    v) Modelling the online safety principles consistently

- Provide underpinning knowledge and behaviours to pupils to help them navigate the online world safely and confidently. Key areas that will be focused on include:
    i) How to evaluate what they see online
    ii) How to recognise techniques used for persuasion
    iii) Online behavior
    iv) How to identify online risks
    v) How and when to seek support

- Recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework ‘Education for a Connected World’ UKCIS (UK Council Internet Safety)
- Lessons for online learning must be carefully planned to ensure that they are age-appropriate and support the learning objectives for specific curriculum areas;
- Remind pupils about their responsibilities through the Pupil Acceptable Use Agreement(s);
- Staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and Trustee training

The Trust:

- makes regular training available to staff regarding e safety issues and the schools’ online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e Safety Policy and the school’s Acceptable Use Agreements.

Parent awareness and training

The Trust:

- provides e safety advice and guidance where applicable

- Promotes e safety through website links

3. Expected Conduct and Incident management

Expected conduct

In our Trust, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff (including supply staff), volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional and reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;
- Monitor pupil usage during lessons and report any concerns regarding individual pupil activity or overall accessibility issues to the internet.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the schools' rules of appropriate use for the whole Trust community are and what sanctions result from misuse.

Incident Management

In our Trust:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions;

- all members of the schools are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school'S escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues;
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing, harrassing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities such as Police and Internet Watch Foundation
- School procedures for dealing with online-safety will be mostly detailed in the following policies:
    - Safeguarding Policy
    - Sexual Harassment Policy
    - Anti-Bullying Policy
    - Behaviour Policy (including school sanctions)
    - Acceptable Use agreement
    - Prevent Policy
    - Data Protection Policy, agreements and other documentation

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*". Furthermore, the Department for Education published the revised statutory guidance Keeping Children Safe in Education 2021 with Annex C.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. All Trust Schools operate the LGFL filtering system (see appendix for LGFL Filter Assessment).

The Trust:

- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;

- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.
- informs all users that Internet/email use is monitored; it is vital that the class teacher and any other adult in the room monitor pupil activity on the internet and report any concerns immediately. Specific staff have access to all accounts, including staff and monitoring is carried out when/ where required.

Network management (user access, backup)

The Trust:

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance; (Trust Sharepoint September 2017)
- Storage of all data within the schools will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, the schools:

- Ensure staff read and sign that they have understood the schools' 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.
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Make 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;
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Require all users to log off when they have finished working or are leaving the computer unattended;
- Ensure all equipment owned by the schools and/or connected to the networks have up to date virus protection;

- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the schools is used primarily to support their professional responsibilities.
- Maintain equipment to ensure Health and Safety is followed;
- Ensure that access to the schools' network resources from remote locations by staff are audited and restricted and access is only through school/LA approved systems:
- Do 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;
- Have a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Use secure data transfer; this includes 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 in our LAs or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password Policy

- The schools make it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the schools should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords that adheres to the Group Password Policy and supports the National Cyber Security Centre suggestion on this area.

E-mail

The schools

- Provide staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing, harassing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Use a number of LGfL-provided technologies to help protect users and systems in the schools, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use LGfL pupil email system which is intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the LGfL e mail system on the school system.
- Staff will use LGfL e-mail systems for professional purposes and must adhere to the Group Email Policy at all times.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher/ Heads of School supported by the Trust Board, take overall responsibility to ensure that the websites are accurate and the quality of presentation is maintained;
- The school websites comply with statutory DFE requirements;
- Most material on the websites are the schools own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school websites;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred systems for such communications.
- Any school approved social networking will adhere to schools' communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher/ Head of School.
- They do not engage in online discussion on personal matters relating to members of the schools community;
- Personal opinions should not be attributed to the school /academy and personal opinions must not compromise the professional role of any staff member, nor bring the Trust into disrepute;
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Breach of any of the above could lead to gross misconduct.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation, harassment including sexual harassment or abuse including sexual abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement. (see appendices for examples used across different Trust Schools).

CCTV

- We have CCTV in the schools as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission. Please see separate CCTV Policy for further detail.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

In this Trust:

- The DCEO is the Senior Information Risk Officer (SIRO) and Group Executive Director Corporate Services is the Trust Data Protection Officer.
- The DCEO, data protection officer and trustees work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Staffs are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to

colleagues or agencies with appropriate permissions. An encrypted non-internal email system is compulsory for sharing pupil data e.g. egress. If this is not possible, the DPO and DSL should be informed in advance.

- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupils & parents or visitors own risk. The Schools accept no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- If a pupil brings his or her mobile phone or personally-owned device into school then it will be handed in at the start of the day. If the device is not handed in and found during the day then it will be confiscated.
- Staff mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / Heads of School. Staff members may only use their personal phones during school break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at another time other than their break times.
- All visitors are requested to keep their phones on silent.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.

- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher/ Heads of School. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher/ Heads of School are able to withdraw or restrict authorisation of use at any time, if it is deemed necessary.
- The Schools reserve the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff school mobile devices may be searched at any time as part of routine monitoring.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office as the phone will be locked away and therefore not answered.
- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- In an emergency such as during lockdown and staff being expected to make safeguarding calls and 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 and then report the incident with the Headteacher / HoS/ Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Digital images and video

In our schools:

- We gain parental/carer permission for use of digital photographs or videos involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials;
- Staff sign the school's 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, high profile use;
- The school blocks/filters access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated and are also taught to consider how to publish for a wide range of audiences which might include Trustees, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils 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 (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying, harassment or abuse.

7. Education at Home

Where children are asked to learn online at home, the Trust has taken into consideration key guidance released by the DfE including 'Safeguarding-in-school-colleges-and-other-providers' and 'safeguarding-and-remote-education'. These are reflected in the COIVD appendices of the Trust Safeguarding policy. Please also see Remote Learning Contingency Plans on school websites to further support this key area.

Appendices

i) Exemplar materials used across schools within the Trust

ii) LGfL Filtering for Education Settings

Visitors and Contractors Acceptable Use Agreement (Exemplar)

Visitors and contractors are asked to sign an Acceptable User Policy (AUP), which outlines how we expect you to behave when you are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media.

Many of these rules are common sense – if you are in any doubt or have questions, please ask.

1. I understand that any activity on a school device or using school networks/platforms/internet may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. If I am given access to school-owned devices, networks, cloud platforms or other technology:
    - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
    - I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role
    - I will not attempt to make contact with any pupils or to gain any contact details under any circumstances
    - I will protect my user name/password and notify the school of any concerns
    - I will abide by the terms of the school Data Protection Policy.
3. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
4. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
5. I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils and will not give any advice on online-safety issues unless this is the purpose of my visit and this is pre-agreed by the school.
6. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the HT/HoS (this may be delegated to other staff) and it will be done in the presence of a member staff.
7. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting / accompanied by: _____

Date / time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

Name / role / date / time: _____

LONDON SOUTH EAST ACADEMIES TRUST

Key Stage 1: Acceptable Use Agreement (Exemplar)

This is how I keep **SAFE online**:

1. I only use the devices I'm **ALLOWED** to	✓
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **KNOW** people online aren't always who they say	
5. I don't keep ~~**SECRETS**~~ just because someone asks me to	
6. I don't change **CLOTHES** in front of a camera	
7. I am **RESPONSIBLE** so never share private information	
8. I am **KIND** and polite to everyone	
9. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
10. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	

My trusted adults are:

_____ **at school**

_____ **at home**

_____

LONDON SOUTH EAST ACADEMIES TRUST

KS2 Pupil Online Acceptable Use Agreement (Exemplar)

This agreement will help keep me safe and help me to be fair to others.

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and remote learning to learn and have fun. I only use apps, sites and games if a trusted adult says I can.
2. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people; I get creative to learn and make things!
3. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
5. ***I am careful what I click on*** – I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. ***I know it's not my fault if I see or someone sends me something bad*** – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell someone.
8. ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
9. ***I know new friends aren't always who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. If I want to meet them, I will ask a trusted adult, and never go alone or without telling an adult.
10. ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
11. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

12. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
13. ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
14. ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
15. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.
16. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
17. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
18. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
19. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes

_____

Outside school, my trusted adults are_____

Signed: _____ **Date: _____**

LONDON SOUTH EAST ACADEMIES TRUST

KS3/4/5 Pupil Acceptable Use Agreement (Exemplar)

1.These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

2. I will treat myself and others with respect at all times; when I am online or using a device, I will treat people in the same way as I would if I were talking to them face to face.
3. Whenever I use technology (a device, the internet, apps, sites and games), I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
4. I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
5. It can be hard to stop using technology sometimes, for adults and young people. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling.
6. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice.
7. If I see anything that shows people hurting themselves or encourages them to do so, I will report it on the app, site or game and tell a trusted adult straight away.
8. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
9. I will work responsibility remotely if I need to and use appropriate apps and resources provided by the school to support my learning.
10. I will only use the school's internet and any device I may be using in school for appropriate school activities and learning, unless I have express permission to carry out recreational activities, e.g. in a lunchtime club or after school.
11. I understand that all internet and device use in school may be subject to filtering and monitoring; school-owned devices may also be subject to filtering and monitoring when used outside of school, and the same expectations apply wherever I am.
12. I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
13. I will not bring files into school or download files that can harm the school network or be used to bypass school security.

14. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
15. I will use the internet, games and apps responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
16. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources (see fakenews.lgfl.net for support).
17. I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside.
18. I will not browse, download, upload, post, share or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
19. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions (many social media sites are 13+) and I should respect this.
20. When I am at school, I will only e-mail or contact people as part of learning activities.
21. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
22. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
23. I will not download copyright-protected material (text, music, video etc.).
24. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
25. Live streaming can be fun but I always check my privacy settings and know who can see what and when. If I live stream, my parents/carers know about it.
26. I will never arrange to meet someone face to face who I have only previously met in an app, site or game without telling and taking a trusted adult with me.
27. I will only use my personal devices (mobile phones, USB devices etc) in school if I have been given permission to do so.
28. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
29. I understand that many apps have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
30. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

31. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
32. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
33. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
34. I know who my trusted adults are at school, home and elsewhere, but if I know I can also get in touch with Childline, The Mix, or The Samaritans.

I have read and understand these rules and agree to them.

Signed: _____ Date:_____

Parent Acceptable Use Agreement (Exemplar)

These rules have been written to help keep everyone safe and happy when you are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

1. I understand that London and South East Academies uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent

comments about others, including the school staff, volunteers, Trustees, contractors, pupils or other parents/carers.

5. I will support my child with remote learning where it is possible to do and I will ask for school advice where necessary to ensure they are able to access appropriate learning resources.
6. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
7. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
8. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
9. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
10. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
11. I can find out more about online safety at London and South East Academies by reading the full Online Safety Policy and can talk to HT/HOS if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

LONDON SOUTH EAST ACADEMIES TRUST

Data Security

Passwords - Do

- use a strong password as per Group Policy (strong passwords are usually 16 characters or more and contain upper and lower case letters, as well as numbers)

Passwords - Don't

- ever share your passwords with anyone else or write your passwords down
- save passwords in web browsers if offered to do so

Laptops - Do

- try to prevent people from watching you enter passwords or view sensitive information
- log-off / lock your 'desktop' when leaving your PC or laptop unattended.

Sending and sharing - Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner(s) if you are not sure. [The SIRO and IAOs need to ask third parties, (if non LA approved), how they will protect sensitive information once it has been passed to them]
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any 'Protected' data outside your school.

Sending and sharing - Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives), if secure remote access is available.
- send sensitive information by email unless it is encrypted; Pupil data must be sent via S2S (DCSF secure web site)

Working on-site - Do

- lock sensitive information away when left unattended, i.e. in lockable drawers, log off or lock work station

Working on site - Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site - Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above

- wherever possible access data remotely instead of taking it off-site - using approved secure authentication – remember GDPR
- make sure you sign out completely from any services you have used
- ensure you save to the appropriate area to enable regular backups
- Ensure safeguarding is highest priority when working remotely with children either during recordings or in live forums.

LONDON SOUTH EAST ACADEMIES TRUST

Guidance: What we do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/ HoS/ DSL and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An inappropriate website is accessed <u>intentionally</u> by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify Trust Board.
4. Inform the school technicians and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
    a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Headteacher/ HoS (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the Headteacher/ HoS should then:
    - Remove the device to a secure place.
    - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (Headteacher/ HoS).
    - Inform Trustees of the incident.

4. In an extreme case where the material is of an illegal nature:
   - Contact the local police and follow their advice.
   - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the Headteacher and Designated Safeguarding Lead.

A bullying/ harassment incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.

2. Secure and preserve any evidence.

3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.

4. Endeavour to trace the origin and inform police as appropriate.

5. Inform LA and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named Designated Safeguard Lead in school and contact parents.

2. Advise the child on how to terminate the communication and save all evidence.

3. Contact CEOP http://www.ceop.gov.uk/

4. Consider the involvement police and social services.

5. Inform LA and other agencies.

6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child

1. Report to and discuss with the named Designated Safeguard Lead in school and contact parents.

2. Advise the child and parents on appropriate games and content.

3. If the game is played within school environment, ensure that the technical team block access to the game

4. Consider the involvement social services and child protection agencies.

5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person

2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.

3. Contact Trust Board

4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Headteacher, HoS and DSL.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

LONDON SOUTH EAST ACADEMIES TRUST

Appropriate Filtering for Education settings

June 2017

Provider Checklist Reponses

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	LONDON GRID FOR LEARNING TRUSTnet London Grid for Learning Known as LGfL, TRUSTnet or LGfL TRUSTnet
Address	LGfL, CI Tower, St George's Square, New Malden, KT3 4TE
Contact details	020 82 555 555 (option 9)
Filtering System	WebScreen™ 2.0 (incorporating NetSweeper and Fortinet technologies)
Date of assessment	11 August 2017

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	

Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
● Are IWF members		LGfL is an engaged IWF member and fully committed to the work, aims and ethos of the Internet Watch Foundation. It makes use of the IWF block lists via Netsweeper, which is the core filtering solution at the heart of WebScreen™ 2.0, the internet filtering solution applied to the LGfL TRUSTnet network.
● and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		The IWF CAIC list is actively implemented by NetSweeper. This is an always-on feature to comply with legislation and ensure safeguarding for school staff and students – it cannot be turned off by schools. In addition, Netsweeper is also one of the first filtering companies to support the Image Hash List, delivering the most effective and efficient solution for combatting the circulation of child sexual abuse images online. Netsweeper ensures that child-abuse imagery which has previously been identified by the IWF will be identified using Microsoft PhotoDNA and blocked if it appears on a new URL. This is important as images are often rehosted after being taken down from their initial URL, and do not disappear, thus perpetualising the abuse. More information on this valuable contribution to the fight against child abuse here.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		This is applied to WebScreen™ 2.0 directly by our support partner Atomwide. This is an always-on feature to comply with legislation and ensure safeguarding for school staff and students – it cannot be turned off by schools.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race,		LGfL's WebScreen™ 2.0 filtering product categorises web content into one or more distinct categories (see Appendix 1), which may (or may not, subject to other local or regional legal obligation or precedent) then be blocked or allowed according to the assigned category/ies,

	religion, age, or sex.		individual URL/s, or the policies defined by the school. Websites unequivocally identified as illegal or a network security risk are automatically categorised and blocked. This cannot be changed by a school. Where a website has been established as potentially inappropriate, however, or if it falls into a high-risk or other category which is blocked by default, a school may take an informed decision to allow these sites in one or more policies. This might be to enable discussion of certain themes in lessons, or where a site's appropriateness may depend upon the age and maturity of users. A range of appropriate, balanced default policies are available to suit the typically differing requirements of primary and secondary schools, for both staff and students, which local school administrators can then modify, by blocking or allowing further categories, websites and webpages, and even applying different profiles to different times of day, different logins, or different computers (e.g. Facebook for teachers but only after 3pm, YouTube for pupils at lunchtime, etc.). The default policies are there to enable informed and proactive safeguarding decisions. Free training courses are offered to all schools to help them best understand and manage the filtering / policy system and interface. Alternatively, an authorised Nominated Contact can request individual category blocking / unblocking requests via the LGfL Support Site. LGfL also has a dedicated Safeguarding Board which works on reviewing the filtering systems from a purely safeguarding perspective. The Board also develops keyword lists based on the latest best-practice and school experience, to aid with up-to-date school-safe and school-appropriate filtering. These keyword lists are added as a further layer over the Google Safe Search functionality, which is turned on by default for all schools. Google's YouTube service is available in the modes: open, moderate restricted and severe restricted. All LGfL default to 'severe-restricted'

			mode, which is recommended. However, schools are permitted to change their settings to use YouTube in 'moderate-restricted' mode. Any school wanting to turn off restricted mode altogether is warned that this is highly inadvisable in an education setting – however, with the approval of the Headteacher, they may bypass DNS settings in order to do so. As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal os.lgfl.net provides a collated and curated portfolio of resources to help teachers, managers, parents and children learn to become effective and safe digital citizens. Many of these resources reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking. Resources are drawn from the entire online-safety community and a variety of providers, but two LGfL resources are particularly relevant in relation to the balancing act of safeguarding vs overblocking: 'Counter-Extremism: narratives and conversations' deals with specific online threats from exposure to extremist material and potential grooming; 'Trust Me' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		See above
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		See above

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		See above
Pornography	displays sexual acts or explicit images		See above
Piracy and copyright theft	includes illegal provision of copyrighted material		See above
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		See above
Violence	Displays or promotes the use of physical force intended to hurt or kill		See above

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects.

WebScreen™ 2.0 utilises the strengths of its underlying technology partners, NetSweeper and Fortinet, but then expands those strengths, and regionalises the results, so that they better suit the UK education sector.

To expand on the capabilities described elsewhere in this response, WebScreen™ 2.0 offers:

Extra 'localised' and specialist web site categories not typically found in commercial filtering, and offering better compatibility with schools' needs.

A devolved hierarchy of central/local policies, that can be adopted and then modified by the local establishment to best suit its particular circumstances, or used in their default state for those with no need or desire to localise the filtered experience.

Data Controller authorisation, which is sought for certain 'high risk' categories, in order to ensure that a full awareness exists within (for instance) a school's Senior Leadership Team, of any polices being deployed that may represent a higher risk than is typically deemed acceptable.

Highly granular settings can enable filtering policies to differentiate between such status as staff and students, locations, times of day, the nature of physical and wireless connections, specific devices by type or ID, and can also conveniently accommodate USO account-holding visitors from other establishments, or non-USO account holding 'Guests' via a range of options.

The service is extremely well documented, and transparent (except where negated by legal or other obligation) in its application of site categorisation and policy application, management and governance.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

WebScreen™ 2.0's content categorisation is a continuous ongoing process, supported by NetSweeper global URL lists and automated AI (artificial intelligence), and underpinned by UKregionalised categorisation obtained using 'crowd-sourced' intelligence from within its own user community.

Local control of policies is actively encouraged, while guidance is provided regarding the need for a balanced approach to filtering being combined with practical and informed support from staff, and the issues that can be encountered by establishments being either too open or too zealous within any given filtering policy.

Where policies are deemed to be effectively appropriate, but needing occasional or temporary exceptions to be applied due to changes in circumstances, WebScreen™ 2.0 policies can be readily modified, and later returned to their otherwise normal state.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		WebScreen™ 2.0 default filter policies are applied appropriate to the underlying nature of a filtered establishment (i.e. Primary School, Secondary School, Teachers' Centre, etc.). Per User filtering is available for deployment across all customer establishments. Multiple filtering policies can be applied, in order to recognise the needs of different groups of users, or locations, or times of day, and/or combinations of each of the above. Filtering policies can be tailored to respond accordingly to different groups of identified individual users, or even a single user.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Yes, fully configurable by appropriately authorised local establishment contacts, or their contracted support agents, via an online portal available 24x7.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Yes, WebScreen™ 2.0 categorises 121 distinct content categories, with descriptions of the purpose and summarised content of each, and where appropriate, the implications of access, and/or prerequisites for gaining access.

● Identification - the filtering system should have the ability to identify users		WebScreen™ 2.0 is fully integrated with the LGfL Shibboleth-compliant IdP, referred to as Unified Sign On (USO), which is run by support partner Atomwide. The system therefore recognises any user presenting a USO ID in response to a filtering policy generated request.

• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		WebScreenTM 2.0 filters any content accessed by http and https protocols, regardless of whether content is browser or application (app) accessible, and is equally applicable to 'mobile' content accessed via an establishment's filtered infrastructure. For mobile apps carrying non-http or https traffic, and which are hence encrypted or 'hidden' against 'content filtering', WebScreen 2.0 can now identify specific apps, or categories of app, analyse their content and collective impact on the local infrastructure, and then where necessary, allow, block or otherwise restrict access according to the wider overall policy or policies applied to the school as a whole. This can be applied to one or more student and staff user groups, and even to individuals, adding a significant dimension over purely http/https filtering, and is hence better suited to combating the recently increasing threats especially in the areas of terrorism, cyber-bullying, and grooming, where apps often attempt to take advantage of this 'invisibility'.
• Multiple language support – the ability for the system to manage relevant languages		Yes, via the NetSweeper embedded technology, WebScreen™ 2.0 supports multi-language filtering.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		No local installed software, nor additional hardware, is required for client devices connected to an establishment's filtered infrastructure.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Yes, via the online management portal, the option to suggest global re-categorisation, or request local re-categorisation, of an individual site or URL, is available to appropriately authorised local establishment contacts, or their contracted support agents.
• Reports – the system offers clear historical information on the websites visited by your users		Yes. A comprehensive range of scheduled, and ad hoc, usage reports is available from the onlinemanagement portal, for use by appropriately authorised local establishment contacts, or their contracted support agents.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Free training courses are offered to all schools to help them best understand and manage the filtering / policy system and interface. Alternatively, an authorised Nominated Contact can submit individual category blocking / unblocking requests via the LGfL Support Site.

LGfL also has a dedicated Safeguarding Board which works on reviewing the filtering systems from a purely safeguarding perspective. The Board also develops keyword lists based on the latest bestpractice and school experience, to aid with up-to-date school-safe and school-appropriate filtering.

As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal os.lgfl.net provides a collated and curated portfolio of resources to help teachers, managers, parents and children learn to become effective and safe digital citizens. Many of these resources reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking.

Resources are drawn from the entire online-safety community and a variety of providers, but two LGfL resources are particularly relevant in relation to the balancing act of safeguarding vs overblocking: 'Counter-Extremism: narratives and conversations' deals with specific online threats from exposure to extremist material and potential grooming; 'Trust Me' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the selfcertification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	John Jackson
Position	Chief Executive Officer
Date	11 August 2017
Signature	*John Jackson*

Appendix 1 – web filtering category list as of 11 August 2017

Please note that this list is subject to change and that definitions of each category and the type of websites likely to be categorised accordingly can be found on the LGfL support site under the WebScreen™ 2.0 menu.

Abortion - Prochoice
Abortion - Prolife
Abortions
Activist/Advocacy Groups
Adult Content
Adult Image
Advertising
Adware
Alcohol
Alternative Lifestyles
Arts & Culture
Bad Link
Banner/Ad Servers
Blogging
Bullying
Classifieds
Computer Security
Criminal Skills
Culinary
Directory
Drugs - Debate
Drugs - Illegal
Drugs - Prescribed
Education
Educational Games
Email
Entertainment
Environmental
Extreme
File Sharing
Forums
Freeware Downloads
Gambling
Games
Gay & Lesbian Issues
General
General News
Hate Speech
Host is an IP
Humor
Images
Infected Hosts
Instant Messaging (IM)
Internet Auction
Intimate Apparel
Intranet Servers
Investing
Job Search
Journals and Blogs
Legal
Malformed URL
Match Making
Matrimonial
Media Protocols
Medical
Medication
Misc Protocols
Music Downloads
Network Unavailable
New URL
No Text
Nudity
Occult
Online Sales
Open Resource Sharing
Parked
Pay to Surf
Peer to Peer
Phishing
Phone Cards
Political
Portals
Profanity
Proxy Anonymizer
Real Estate
Redirector Page
Religion
Ringtones
Safe Search
Sales
Search Engine
Search Keywords
Security Threat
Self Help
Sex Education
SMS Messaging
Social Issues and Support
Social Networking
Sport - Hunting and Gun Clubs
Sports
Streaming Media
Substance Abuse
Tasteless/Illegal/Questionable
Technology
Tobacco
Travel
Under Construction
URL Translation
Violence
Viruses
Voice Over IP (VOIP)
Weapons
Web Chat
Web E-mail
Web Hosting
Web Storage
Web-Based Chat & Email