

+-



# London South East Academies Trust

---

## E-Safety Policy

<b>Responsible post holder</b>	Executive Headteacher
<b>Approved by / on</b>	1 <sup>st</sup> July 2017
<b>Reviewed</b>	1 <sup>st</sup> September 2018
<b>Next Review</b>	1 <sup>st</sup> September 2019

**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

### 1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

### 2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

### 3. Expected Conduct and Incident Management

### 4. Managing the IT Infrastructure

- Internet access, security (virus protection), filtering and monitoring
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

### 5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

## 6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

### **Appendices (separate documents):**

- A1: Acceptable Use Agreement (Staff, Volunteers and Governors)
- A2: Acceptable Use Agreements (Pupils – adapted for phase)
- A3: Acceptable Use Agreement including photo/video permission (Parents)
- A4: Protocol for responding to online safety incidents  
<http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx> - handling infringements  
<http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf> - page 23 onwards
- A5: Prevent: Radicalisation and Extremism
- A6: Data security: Use of IT systems and Data transfer  
Search and Confiscation guidance from DfE  
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>
- A7: **Guidance: What we do if?**
- A8: 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.
- 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 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

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

#### Conduct

- Aggressive behaviours (bullying)
- 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)

## Scope

This policy applies to all members of **London South East Academies Trust** including staff, 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
Executive Headteacher/ Heads of School	<ul style="list-style-type: none"> <li>• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance</li> <li>• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding</li> <li>• To take overall responsibility for online safety provision</li> <li>• To take overall responsibility for data management and information security ensuring school provisions follow best practice in information handling</li> <li>• To ensure the schools use appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services</li> <li>• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles</li> <li>• To be aware of procedures to be followed in the event of a serious online safety incident</li> <li>• To ensure Trustees are regularly updated on the nature and effectiveness of the schools' arrangements for online safety</li> <li>• To ensure school websites include relevant information.</li> </ul>
Designated E-Safety Child Protection Lead	<ul style="list-style-type: none"> <li>• Lead role in establishing and reviewing the schools' online safety policy/documents</li> <li>• Promote an awareness and commitment to online safety throughout the Trust community</li> <li>• Ensure that online safety education is embedded within the curriculum for all settings</li> <li>• Liaise with school technical staff where appropriate across the Trust</li> <li>• To communicate regularly with SLT, EHT and the designated online safety Trustee to discuss current issues, review incident logs and filtering</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident</li> </ul>

Role	Key Responsibilities
	<ul style="list-style-type: none"> <li>• To ensure that online safety incidents are logged as a safeguarding incident</li> <li>• Facilitate training and advice for all staff</li> <li>• Oversee any pupil surveys / pupil feedback on online safety issues</li> <li>• Liaise with the Local Authority and relevant agencies</li> <li>• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.</li> </ul>
Trustee (E Safety)	<ul style="list-style-type: none"> <li>• To ensure that the school has in place policies and practices to keep the children and staff safe online</li> <li>• To approve the E Safety Policy and review the effectiveness of the policy</li> <li>• To support the schools in encouraging parents and the wider community to become engaged in online safety activities</li> <li>• The role of the E safety Trustee will include a regular review with the Designated E Safety Lead.</li> </ul>
ICT Curriculum Leader	<ul style="list-style-type: none"> <li>• To oversee the delivery of the online safety element across the curriculum for each school</li> </ul>
Network Manager/technician	<ul style="list-style-type: none"> <li>• To report online safety related issues that come to their attention, to the Designated E Safety Lead, SLT and EHT</li> <li>• To manage the schools' computer systems, ensuring <ul style="list-style-type: none"> <li>- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)</li> <li>- access controls/encryption exist to protect personal and sensitive information held on school-owned devices</li> </ul> </li> <li>• 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</li> <li>• That the use of schools technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to Heads of School/ EHT.</li> <li>• To ensure appropriate backup procedures and disaster recovery plans are in place</li> <li>• To keep up-to-date documentation of the school's online security and technical procedures</li> </ul>
LGfL Nominated contact(s)	<ul style="list-style-type: none"> <li>• To ensure all LGfL services are managed on behalf of the schools following data handling procedures as relevant</li> </ul>

Role	Key Responsibilities
Teachers	<ul style="list-style-type: none"> <li>• To embed online safety in the curriculum</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant)</li> <li>• 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</li> <li>• To monitor online behaviour in class and report any concerns to appropriate SLT</li> </ul>
All staff, volunteers and contractors.	<ul style="list-style-type: none"> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction</li> <li>• To report any suspected misuse or problem to the Designated Lead</li> <li>• To maintain an awareness of current online safety issues and guidance e.g. through CPD</li> <li>• To model safe, responsible and professional behaviours in their own use of technology</li> </ul> <p><b>Exit strategy</b></p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Pupils	<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually</li> <li>• To understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology</li> <li>• To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the schools' online safety policy covers their actions out of school</li> <li>• To contribute to any 'pupil voice' / surveys that gathers information of their online experiences</li> </ul>

Role	Key Responsibilities
Parents/carers	<ul style="list-style-type: none"> <li>• To read, understand and promote the schools' Pupil Acceptable Use Agreement with their children</li> <li>• to consult with the schools if they have any concerns about their children's use of technology</li> <li>• to support the schools in promoting online safety including the pupils' use of the Internet and the schools' use of photographic and video images</li> </ul>
External groups including Parent groups	<ul style="list-style-type: none"> <li>• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within schools</li> <li>• to support the schools in promoting online safety</li> <li>• To model safe, responsible and positive behaviours in their own use of technology.</li> </ul>

### Communication:

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

- Policy to be posted on the schools websites
- 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 will act as first point of contact for any incident
- Any suspected online risk or infringement is reported to Designated Lead on that day
- Any concern about staff misuse is always referred directly to the Executive Headteacher, unless the concern is about the Executive Headteacher in which case the complaint is referred to the Chair of Trust 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, 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 2018.
- 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 Trust:

- has an online safety education programme as part of the ICT curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Lesson plans for online learning must be carefully planned to ensure that they are age-appropriate and support the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures 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;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures 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:

- runs a programme of e safety advice, guidance and training for parents.
- 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, 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 schools' 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, IWF) 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 schools;
- 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 or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

#### **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’ 3rd September 2018 for schools and colleges in England. Key information can be found in KCSIE 2018 Annex C: Online Safety.

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 the class teacher and any other adult in the room to 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;
- Uses teacher 'remote' management control tools at BTA Hayes Campus for controlling workstations/viewing users' for BTA sites
- 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](#); ( for 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' online 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 LA 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;

### **Passwords**

- 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.

### **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 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.
- 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 Executive Headteacher, supported by the Trust Board, takes overall responsibility to ensure that the websites are accurate and the quality of presentation is maintained;
- The school websites complies 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 Executive Headteacher.
- 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 or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

#### **CCTV**

- We have CCTV in the school 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 Executive Headteacher is the Senior Information Risk Officer (SIRO) and Group Executive Director Corporate Services is the Trust Data Protection Officer.
- 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 Executive 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 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 Executive Headteacher/ Heads of School. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Executive 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 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 Executive Headteacher / HoS/ Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

### **Storage, Syncing 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 synced 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 or abuse.

# Appendices

## Staff, Trustee and Visitor Acceptable Use Agreement /Code of Conduct

Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources**, learning platform, software, communication tools, social networking tools, school website, **equipment and systems**.

The Trust regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

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.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will only use the approved *email system, Learning Platform, online cloud storage service and school approved communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager / school named contact*.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

- I will follow the school's policy on use of mobile phones / devices at school and *will not take into classrooms / only use in staff areas*.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will only I take or publish images of staff and pupils with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify pupils by name, or other personal information.
- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the Trust approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert [*the schools named*] Child Protection lead / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to *senior member of staff / designated Child Protection lead*.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to *the Head / Safeguarding Lead* on their request.
- I understand that Internet encrypted content, may be scanned for security and/or safeguarding purposes.
- I will only use any Trust system I have access to in accordance with their policies.
- Staff that have a teaching role only: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

### **User Signature**

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date.....

Full Name ..... (printed)

Job title / Role .....

**Authorised Signature (Head Teacher / Deputy)**

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date.....

Full Name ..... (printed)



# Key Stage 1: Acceptable Use Agreement

Keep **SAFE** online because ...

## TRUST



I **CHECK** it's OK to use a website / game / app.

I **ASK** for help if I get lost online.

I **THINK** before I click on things.

I **KNOW** online people are really strangers.

I am **RESPONSIBLE** so never share private information.

I am **KIND** and polite online.

I **TELL** a trusted adult if I am worried about anything.

My trusted adults are:

Mum

Dad

Teacher

My name:

Date signed:

--

## KS2 Pupil Online Acceptable Use Agreement

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

- ***I am an online digital learner*** – I use the school’s IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people’s work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to ‘double check’ all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

**I have read and understood this agreement.**

**I know who are my trusted adults are and agree to the above.**

Signed:

Date:

---

---

### KS3/4/5 Pupil Acceptable Use Agreement

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.

1. I will be a responsible user and stay safe when using the internet and other digital technology at school.
2. I will only use the school's computers for appropriate school activities and learning and I am aware that the school can monitor my internet use.
3. I will not use school systems and equipment for personal and recreational use unless I have permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
6. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
7. I will use the Internet responsibly and will not visit websites that are inappropriate for the school or my learning activities.
8. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
9. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions and I should respect this.
10. I will only e-mail or contact people as part of learning activities.
11. 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.
12. 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.
13. When using the internet, I will not download copyright-protected material (text, music, video etc.)
14. 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.
15. I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.
16. I will only use my personal devices (mobile phones, USB devices etc.,) in school if I have been given permission to do so.
17. 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.
18. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

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

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Data Security

### Passwords - Do

- use a strong password (strong passwords are usually eight 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

## Guidance: What we do if?

**An inappropriate website is accessed unintentionally in school by a teacher or child.**

1. Play the situation down; don't make it into a drama.
2. Report to the Executive Headteacher/ HoS/ e- safety officer 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 intentionally 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 intentionally 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 Executive 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 Executive 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 (Executive Headteacher).
  - 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 Executive Headteacher and online-safety officer.

**A bullying 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](http://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 Executive Headteacher, HoS and online-safety officer.

**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 Grid for Learning Provider Checklist

Company / Organisation	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	17 June 2016

### 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	

### Illegal Online Content

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

Aspect	Rating	Explanation
<ul style="list-style-type: none"> <li>Are IWF members</li> </ul>		WebScreen™ 2.0, the internet filtering solution applied to the LGfL TRUSTnet network, uses URL filtering from NetSweeper and Fortinet, which are both IWF members. Furthermore, LGfL is currently exploring closer partnership working with the IWF.
<ul style="list-style-type: none"> <li>and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)</li> </ul>		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 pupils – it cannot be turned off by schools.
<ul style="list-style-type: none"> <li>Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li> </ul>		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 pupils – 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, religion, age, or sex.		<p>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, individual URL/s, or the policies defined by the school.</p> <p>Websites unequivocally identified as illegal or a network security risk are automatically categorised and blocked. This cannot be changed by a school.</p> <p>Where a website has been established as <u>potentially</u> 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.</p>

		<p>A range of appropriate, balanced default policies are available to suit the typically differing requirements of primary and secondary schools, for both staff and pupils, 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.</p> <p>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.</p> <p>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.</p> <p>These keyword lists are added as a further layer over the Google Safe Search functionality, which is turned on by default for all schools.</p> <p>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.</p> <p>As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal <a href="https://os.lgfl.net">os.lgfl.net</a> 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</p>
--	--	--

			<p>reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking.</p> <p>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: '<a href="#">Counter-Extremism: narratives and conversations</a>' deals with specific online threats from exposure to extremist material and potential grooming; '<a href="#">Trust Me</a>' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).</p>
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		See above

	of physical force intended to hurt or kill		
--	--	--	--

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 pupils, 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 UK-regionalised 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
<ul style="list-style-type: none"> <li>Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role</li> </ul>	<p style="text-align: center;">A</p>	<p>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.).</p> <p>Per User filtering is available for deployment across all customer establishments.</p> <p>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.</p> <p>Filtering policies can be tailored to respond accordingly to different groups of identified individual users, or even a single user.</p>
<ul style="list-style-type: none"> <li>Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content</li> </ul>	<p style="text-align: center;">A</p>	<p>Yes, fully configurable by appropriately authorised local establishment contacts, or their contracted support agents, via an online portal available 24x7.</p>
<ul style="list-style-type: none"> <li>Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking</li> </ul>	<p style="text-align: center;">A</p>	<p>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.</p>

<ul style="list-style-type: none"> <li>● Identification - the filtering system should have the ability to identify users</li> </ul>		<p>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.</p> <p>The system therefore recognises any user presenting a USO ID in response to a filtering policy generated request.</p>
<ul style="list-style-type: none"> <li>● Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies</li> </ul>		<p>WebScreen™ 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.</p>
<ul style="list-style-type: none"> <li>● Multiple language support – the ability for the system to manage relevant languages</li> </ul>		<p>Yes, via the NetSweeper embedded technology, WebScreen™ 2.0 supports multi-language filtering.</p>
<ul style="list-style-type: none"> <li>● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices</li> </ul>		<p>No local installed software, nor additional hardware, is required for client devices connected to an establishment's filtered infrastructure.</p>
<ul style="list-style-type: none"> <li>● Reporting mechanism – the ability to report inappropriate content for access or blocking</li> </ul>		<p>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.</p>

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*”.<sup>3</sup>

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 best-practice 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](http://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 self-certification 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	20 June 2016