

# ONLINE SAFETY POLICY



## CITY OF LONDON ACADEMY

**Responsibility:** Designated Safeguarding Lead

**Last Approved by Governors:** new

**Next Approval by Governors:** Due April 2018

**Next Review date:** March 2019

**This policy is part of the Academy's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the Academy'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) and filtering
  - Network management (user access, backup, curriculum and admin)
  - Passwords policy
  - E-mail
  - Academy 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

## 1. Introduction and Overview

### Rationale

#### The purpose of this policy is to:

- Set out the key principles expected of all members of the Academy community at The City of London Academy 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 Academy community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other Academy policies].
- Ensure that all members of the Academy 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 students.

#### The main areas of risk for our Academy 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
- Copyright (little care or consideration for intellectual property and ownership)

### Scope

This policy applies to all members of the City of London Academy community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of the academy IT systems, both in and out of the City of London Academy. The Education and Inspections Act 2006 empowers Headteachers, to such an extent as is reasonable, to regulate the

behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

### Roles and responsibilities

Role	Key Responsibilities
Head 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 (SIRO) ensuring the Academy's provision follows best practice in information handling</li> <li>● To ensure the Academy uses 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>● Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised</li> <li>● To receive regular monitoring reports from the Online Safety Coordinator</li> <li>● To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager</li> <li>● To ensure Governors are regularly updated on the nature and effectiveness of the Academy's arrangements for online safety</li> <li>● To ensure the Academy website includes relevant information.</li> </ul>
Online Safety Co-ordinator	<ul style="list-style-type: none"> <li>● Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the Academy's online safety policy/documents</li> <li>● Promote an awareness and commitment to online safety throughout the Academy community</li> <li>● Ensure that online safety education is embedded within the curriculum</li> <li>● Liaise with Academy technical staff where appropriate</li> <li>● To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs</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> <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>

Governors	<ul style="list-style-type: none"> <li>● To ensure that the Academy has in place policies and practices to keep the children and staff safe online</li> <li>● To approve the Online Safety Policy and review the effectiveness of the policy</li> <li>● To support the Academy in encouraging parents and the wider community to become engaged in online safety activities</li> <li>● The role of the online safety Governor will include: regular review with the online safety Coordinator</li> </ul>
ICT Curriculum Lead	<ul style="list-style-type: none"> <li>● To oversee the delivery of the online safety element of the Computing curriculum</li> </ul>
Network Manager	<ul style="list-style-type: none"> <li>● To report online safety related issues that come to their attention, to the Online Safety Coordinator</li> <li>● To manage the Academy's computer systems, ensuring <ul style="list-style-type: none"> <li>- Academy password policy is strictly adhered to.</li> <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 Academy-owned devices</li> <li>- the Academy's policy on web filtering is applied and updated on a regular basis</li> </ul> </li> <li>● That they keep up to date with the Academy's online 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 Academy technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety Coordinator/Headteacher</li> <li>● To ensure appropriate backup procedures and disaster recovery plans are in place</li> <li>● To keep up-to-date documentation of the Academy's online security and technical procedures</li> </ul>
Data and Information (Asset Owners) Managers (IAOs)	<ul style="list-style-type: none"> <li>● To ensure that the data they manage is accurate and up-to-date</li> <li>● Ensure best practice in information management. I.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.</li> <li>● The Academy must be registered with Information Commissioner</li> </ul>
LGfL Nominated contact(s)	<ul style="list-style-type: none"> <li>● To ensure all LGfL services are managed on behalf of the Academy following data handling procedures as relevant</li> </ul>
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> </ul>

<p>All staff, volunteers and contractors.</p>	<ul style="list-style-type: none"> <li>● To read, understand, sign and adhere to the Academy 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 online safety coordinator</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 Academy. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to login and allow a factory reset.</li> </ul>
<p>Students</p>	<ul style="list-style-type: none"> <li>● Read, understand, sign and adhere to the Student/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 Academy's 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>
<p>Parents/carers</p>	<ul style="list-style-type: none"> <li>● To read, understand and promote the Academy's Pupil Acceptable Use Agreement with their child (ren)</li> <li>● to consult with the Academy if they have any concerns about their children's use of technology</li> <li>● to support the Academy in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the Academy's use of photographic and video images</li> </ul>
<p>External groups including Parent groups</p>	<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 the Academy</li> <li>● to support the Academy in promoting online safety</li> <li>● To model safe, responsible and positive behaviours in their own use of technology.</li> </ul>

## **Communication:**

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

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

## **Handling Incidents:**

- The Academy will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which the case is referred to the Chair of Governors and the LADO (Local Authority Designated Officer).

## **Handling a sexting / nude selfie incident:**

[UKCCIS "Sexting in schools and colleges"](#) should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people  
*When assessing the risks the following should be considered:*
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual

- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the Academy's pastoral support and disciplinary framework and if appropriate local network of support.

### **Reviewing and Monitoring Online Safety**

The online safety policy is referenced within other Academy policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Academy
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the Academy online safety policy will be disseminated to all members of staff and pupils.

## **2. Education and Curriculum**

### **Pupil online safety curriculum**

This Academy:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students 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;
- ensure pupils only use Academy-approved systems and publish within appropriately secure / age-appropriate environments.

### **Staff and governor training**

This Academy:

- makes regular training available to staff on online safety issues and the Academy's online safety education programme;
- 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 Online Safety Policy and the Academy's Acceptable Use Agreements.

### **Parent awareness and training**

This Academy:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

### 3. Expected Conduct and Incident management

#### Expected conduct

In this Academy, all users:

- are responsible for using the Academy 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 reporting 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 the Academy;
- know and understand Academy 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 uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, 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;

#### 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 Academy's 'rules of appropriate use for the whole Academy community' are and what sanctions result from misuse.

## **Incident Management**

In this Academy:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the Academy are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the Academy'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, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the Academy;
- 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**

This Academy:

- informs all users that Internet/email use is monitored;
- 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 students.

### **Network management (user access, backup)**

This Academy

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services; although this is kept to a minimum
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- 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 frequent back-ups of Academy data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the Academy 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, this Academy:

- Ensures staff read and sign that they have understood the Academy's 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;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has 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;
- Requires all users to log off when they have finished working or are leaving the computer unattended. Enforced by locking screens after a timeout which requires them to log back in if they are still using the equipment
- Ensures all equipment owned by the Academy and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Academy, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;  
e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote offsite backup of critical data;
- This Academy uses secure data transfer; this includes DfE secure S2S website or Google Drive (which has its own security) for all CTF files sent to other Academies;
- 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
- 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**

- This Academy makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the Academy should be notified immediately.
- All staff have their own unique username and private passwords to access Academy systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, according to the Multi Academy Trust password policy.
- We have enabled staff using critical systems to use two factor authentication.

### **E-mail**

#### **This Academy**

- Provides staff with an email account for their professional use, Google Mail;
- We use anonymous or group e-mail addresses where possible, for example [info@schoolname.la.sch.uk](mailto:info@schoolname.la.sch.uk)/[head@schoolname.la.sch.uk](mailto:head@schoolname.la.sch.uk)
- 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.
- We use a number of technologies to help protect users and systems in the Academy, including desktop anti-virus product Sophos and monitoring/safeguarding software Impero.

#### **Pupils:**

- Pupils are taught about the online safety and 'etiquette' of using e-mail both in the Academy and at home.

#### **Staff:**

- Staff can only use the Google Email system within the Academy
- Access in Academy to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data outside of the Academy. '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.

#### **Academy website**

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The Academy website complies with statutory DFE requirements;
- Most material is the Academy's 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 Academy website;

#### **Cloud Environments**

- In Academy, pupils are only able to upload and publish within Academy approved 'Cloud' systems.

## **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 student use on a personal basis or to open up their own spaces to their students, but to use the Academy's preferred system for such communications.
- for the use of any Academy approved social networking will adhere to Academy's communications policy.

### **Academy staff will ensure that in private use:**

- No reference should be made in social media to students/pupils, parents/carers or Academy staff;
- Academy staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the Academy community;
- Personal opinions should not be attributed to the Academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the Academy into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

#### **Pupils:**

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

#### **Parents:**

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

## **CCTV**

- We have CCTV in the Academy as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the Academy. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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

### **Strategic and operational practices**

At this Academy:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key Academy information (the Information Asset Owners) are. We have listed the information and information asset owners.

- 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.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all Academy-owned hardware will be recorded in a hardware inventory.
- Details of all Academy-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.
- We are using secure file deletion software.

## 6. Equipment and Digital Content

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

- Mobile devices brought into the Academy are entirely at the staff member, students & parents or visitors own risk. The Academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into the Academy.
- Mobile devices brought in to the Academy are the responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. 'Mobile-free' signs to this effect are displayed.
- All mobile devices will be handed in at reception should they be brought into school.
- Personal mobile devices will not be used during lessons or formal teaching time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, which are brought into the Academy, must be turned off (not placed on silent) and stored out of sight on arrival at the Academy. They must remain turned off and out of sight until the end of the day.
- 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.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during Academy break times.
- All visitors are requested to keep their phones on silent.
- 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. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The Academy reserves the right to search the content of any mobile devices on the Academy premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- If a student needs to contact his or her parents or carers, they will be allowed to use an Academy phone. Parents are advised not to contact their child via their mobile phone during the Academy day, but to contact the Academy office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the Academy office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

## **Storage, Syncing and Access**

### **The device is accessed with an Academy owned account**

- The device has an Academy 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 an Academy owned mobile device, staff must be aware that the Academy use will be synced to their personal cloud, and personal use may become visible in the Academy 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.

## **Students' use of personal devices**

- The Academy strongly advises that student mobile phones and devices should not be brought into Academy.
- The Academy accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the Academy policy, then the device will be confiscated and will be held in a secure place in the Academy office. Mobile devices will be released to parents or carers in accordance with the Academy policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

## **Staff use of personal devices**

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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 students 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 Headteacher / Designated Officer.
- If a member of staff breaches the Academy policy then disciplinary action may be taken.

## **Digital images and video**

### **In this Academy:**

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the Academy agreement form when their daughter/son joins the Academy (or annually).;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Academy produced video materials/DVDs;
- Staff sign the Academy'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 Academy web site, in the prospectus or in other high profile publications the Academy will obtain individual parental or pupil permission for its long term, high profile use
- The Academy blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing 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.

**Policy Ratified / Approved:**

\_\_\_\_\_ **Chair of Governors** \_\_\_\_\_ **Date**

\_\_\_\_\_ **Head of School** \_\_\_\_\_ **Date**

\_\_\_\_\_ **Designated Safeguarding Lead** \_\_\_\_\_ **Date**

Appendices (download these documents as a zip file from [osappendices.lgfl.net](http://osappendices.lgfl.net)):

- 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>