EMPOWER
LEARNING ACADEMY TRUST

Online-Safety Policy

Agreed by: C.E.O. *

Review Date: July 2024

EMPOWER LEARNING ACADEMY TRUST

Online-Safety Policy

CONTENTS

Overview **1**
- Aims 1
- Scope 1

Roles and responsibilities **2**
- Headteacher / Principal 2
- Designated Safeguarding Lead / Online-Safety Lead 3
- Governing Body, led by Safeguarding Governor 4
- All staff 6
- PSHE(E) leads 7
- Computing curriculum lead(s) 7
- Subject / aspect leaders 7
- Network Manager / technician 8
- Data Protection Officer (DPO) 9
- LGfL TRUSTnet Nominated contacts 9
- Volunteers and contractors 9
- Pupils 10
- Parents/carers 11
- External groups including parent associations 11

Education and curriculum **11**

Handling online-safety concerns and incidents **12**

Appropriate filtering and monitoring **13**

Communication **13**
- Email and messaging 13

Academy websites **14**

Cloud platforms **14**

Digital images and video **15**

Social media **16**
- Staff, pupils' and parents' social media presence 16

Device usage **17**
- Personal devices and bring your own device (BYOD) policy 17
- Network / internet access on personal devices 19
- Trips / events away from the academy 19
- Searching and confiscation 19

Key online-safety staff **20**
- Bower Park Academy 20
- Hall Mead School 20
- The Brittons Academy 20
- Hacton Primary School 20

Related documents and references **21**

Online-Safety Policy

Overview

This policy is based on the London Grid for Learning DigiSafe template, drawing on research and expertise from the Department for Education and the LGfL DigiSafe survey of 40,000 pupils.

Aims

This policy aims to:

- Set out expectations for all ELAT community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online / digital behaviour standards (including social media activity) must be upheld beyond the confines of the academy gates and school day, regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help academy staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the academy, supporting the ethos, aims and objectives of the Trust, and protecting the reputation of the academy and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to related policies)

Scope

This policy applies to all members of the ELAT community (including staff, governors, volunteers, contractors, students / pupils, parents / carers, visitors and community users) who have access to digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and responsibilities

Each Empower Learning Academy Trust (ELAT) academy is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the academy. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher / Principal

Key responsibilities

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding team and ensure that the Designated Safeguarding Lead (DSL) responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on academy issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the academy's provision follows best practice in information handling; working with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the academy implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online-safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised

- Ensure that there is a system in place to monitor and support staff (e.g. the network manager who carries out technical procedures related to online-safety)
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the academy website meets statutory DfE requirements (see appendices)

Designated Safeguarding Lead / Online-Safety Lead

Key responsibilities

(all quotes below are from the Department for Education's (DfE) 'Keeping Children Safe in Education 2019')

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)., this lead responsibility should not be delegated"
- Work with the Headteacher/Principal and technical staff to review protections for **pupils in the home** [Smoothwall Monitor, Senso.Cloud, Meraki MDM] and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Where the online-safety coordinator is not the named DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with 'Working Together to Safeguard Children'" (DfE)
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher (if relevant), DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy and other related documents (e.g. Acceptable Use Policies) to ensure a joined-up approach to online safety
- Receive regular updates in online-safety issues and legislation, be aware of local and academy trends
- Ensure that online-safety education is embedded across the curriculum (e.g. by use of the UKCCIS framework 'Education for a Connected World') and beyond, in wider school life

- Promote an awareness and commitment to online safety throughout the academy community, with a strong focus on parents, including hard-to-reach parents
- Liaise with academy technical, pastoral, and support staff as appropriate
- Communicate regularly with senior leaders and the designated online safety governor / committee to discuss current issues (anonymised), review incident logs and discuss the effectiveness of filtering and monitoring
- Ensure that all staff are aware of the procedures they should follow in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss filtering and monitoring (physical or technical) with governors and ensure staff are aware that these safeguards are in place
- Ensure that the 2018 DfE guidance on sexual violence and harassment is followed throughout the academy and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read 'Keeping Children Safe in Education' Part 1 and all those working with children Annex A
    - staff are encouraged to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation

Trust Board, led by Safeguarding Trustee

Key responsibilities

(all quotes below are from the DfE's 'Keeping Children Safe in Education 2019')

- Approve this policy and strategy and subsequently review its effectiveness
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Ensure an appropriate senior member of staff, from each of the academy leadership team's, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority.
- Support the academies in encouraging parents and the wider community to become engaged in online- safety activities
- Have regular strategic reviews with the online-safety co-ordinators / DSL's and incorporate online safety into standing discussions of safeguarding at Local Governance Committee (LGC) meetings

- Where the online-safety coordinator is not the named DSL, ensure that there is regular review and open communication between these roles

- Work with the DPO, DSLs and headteachers to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

- Check all academy staff have read Part 1 of 'Keeping Children Safe in Education'; SLT and all staff working directly with children have read Annex A; check that Annex C on online safety reflects practice in academy

- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and are regularly updated in line with advice from the LSCB (Local Safeguarding Children Board)

- Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology."

All staff

Key responsibilities

- Pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies** (see coronavirus.lgfl.net/safeguarding for an infographic overview of safeguarding considerations for remote teaching technology. There are further details in the staff AUP.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections)
- Read and follow this policy in conjunction with the academy's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report it in accordance with academy procedures
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct / handbook
- Notify the DSL / OSL if policy does not reflect practice in your academy and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all academy activities, both outside the classroom and within the curriculum, supporting curriculum / stage / subject leads and making the most of unexpected learning opportunities as they arise
- Whenever overseeing the use of technology in academy, remote teachingor homework tasks, encourage sensible use, monitor what pupils / students are doing and consider potential dangers and the age appropriateness of websites
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the **20 Safeguarding Principles for Remote Lessons** infographic which applies to all online learning Carefully supervise and guide pupils when engaged in learning activities that involve online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, as well as legal issues such as copyright and data law
- Encourage pupils / students to follow their acceptable use policy, remind them about it and enforce academy sanctions
- Notify the DSL / OSL of new trends and issues before they become a problem

- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL / OSL know
- Receive regular updates from the DSL / OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in the use of technology. This includes outside of the academy's hours, offsite and on social media, in all aspects upholding the reputation of the academy and the professional reputation of all staff

PSHE(E) leads

Key responsibilities from September 2019 for September 2020
(quotes taken from DfE press release on 19 July 2018 on 'New relationships and health education in schools')

As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE(E) curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL / OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE(E)

Computing curriculum lead(s)

Key responsibilities

As listed in the 'all staff' section, plus:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL / OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in the academy's to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities

As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in your subject and model positive attitudes and approaches to staff and pupils alike

- Consider how the UKCCIS framework 'Education for a Connected World' can be applied in your context
- Work closely with the DSL / OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Network Manager / technician

Key responsibilities

As listed in the 'all staff' section, plus:

- Support the Headteacher/Principal and DSL team as they review protections for **pupils in the home** [Smoothwall Monitor, Senso.Cloud, Meraki MDM] and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Keep up to date with the Trust's online-safety policy and technical information in order to effectively carry out the online safety role and inform and update others as relevant
- Work closely with the DSL / OSL, Data Protection Officer (DPO) and LGfL TRUSTnet nominated contacts to ensure that academy systems and networks reflect academy's policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal data, web filtering settings, sharing permissions for files on cloud platforms etc)
- Support and advise on the implementation of appropriate filtering and monitoring as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the academy's online security and technical procedures
- To report online-safety related issues that come to their attention in line with the Trust's policies
- Manage the academy's systems, networks and devices, according to a strict password policy, with systems in place to detect misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of academy technology, online platforms and social media presence and ensure that misuse / attempted misuse is identified, reported and managed in line with school policy
- Work with the Headteacher to ensure that the academy website meets statutory DfE requirements

Data Protection Officer (DPO)

Key responsibilities

- Be aware of the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
    - "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding"
- The same document states that the retention schedule for safeguarding records may be required to be set as "Very long term need (until pupil is aged 25 or older)"
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and for safeguarding information sharing as outlined above
- Ensure that all access to safeguarding data is limited as appropriate as well as monitored and audited

LGfL TRUSTnet Nominated contacts

Key responsibilities

- To ensure all LGfL TRUSTnet services are managed on behalf of the academy in line with ELAT policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure that they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications for online-safety of all existing services and changes to settings that might be requested

Volunteers and contractors

Key responsibilities

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the DSL / OSL
- Maintain an awareness of current online-safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities

- Read, understand, sign and adhere to the student / pupil acceptable use policy
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of the academy and realise that the academy's acceptable use policies cover actions out of school, including on social media
- Understand the benefits / opportunities and risks / dangers of the online world and know who to talk to at school or outside of school if there are problems

Parents/carers

Key responsibilities

- Read, sign and promote the academy's parental acceptable use policy and read the pupil acceptable use policy and encourage their children to follow it
- Consult with the academy if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative or threatening comments about others, including members of the academy community
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

External groups including parent associations

Key responsibilities

- Any external individual / organisation will sign an acceptable use policy prior to using technology or the internet within the academy
- Support the academy in promoting online safety and data protection
- Model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative or threatening comments about others, including members of the school community

Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE(E)
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all of the academy's activities, both outside the classroom and within the curriculum, supporting curriculum / stage / subject leads and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology in the academy or setting a homework task, all staff should encourage sensible use and consider potential dangers as well as the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting as well as legal issues such as copyright and data law.

At ELAT we recognise that online safety and broader digital resilience must be threaded throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCCIS (the UK Council for Child Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE(E), Citizenship and (from September 2019 for September 2020) the statutory Health Education and Relationships Education (for secondaries: Relationships and Sex Education).

General concerns must be handled in the same way as any other safeguarding concern; all stakeholders should talk to the DSL / OSL with even the smallest concern. This could contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

The Trust's procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy and Procedures
- Behaviour and Attendance Policy
- Acceptable Use Policies
- Data Protection Policy

Each academy commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside and outside of the academy (and that those from outside may continue to impact on pupils when they come into the academy). All members of the academy are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the escalation processes.

Any suspected online risk or infringement should be reported to the OSL / DSL on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern / allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the Local Authority's Designated Officer (LADO). Staff may also use the NSPCC Whistleblowing Advice Line.

The academy will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). Parents / carers will be informed of online-safety incidents involving their children. The Police will be contacted where staff or pupils engage in or are subject to behaviour which may be considered particularly disturbing or breaks the law.

Appropriate filtering and monitoring

'Keeping Children Safe in Education' obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

ELAT academies use the internet connection provided by LGfL TRUSTnet. This means all academies have a dedicated, secure, school-safe connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

In each of our academies we always use one or more of the methods listed above, based on context.

Communication

Email and messaging

- Pupils at the academy use approved systems for all school emails (Office 365 or Gmail as part of GSuite for Education)
- Staff only use Office 365 and school-managed messaging systems for academy business

These systems are managed by the academies and, in the case of LGfL, are auditable and trackable by LGfL TRUSTnet on behalf of the school.

General principles for email and messaging are as follows:

- Academy email systems and messaging within learning environments managed by academies are the only means of electronic communication to be used between staff and pupils or staff and parents (in both directions). Any unauthorised use of a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member). There should be no circumstances where a private email or messaging is used.

- Staff or pupil personal data should never be sent / shared / stored on email.

    - If data needs to be shared with external agencies, it should be send encrypted using a password protected zip file. Internally, staff should use the academy's network, including when working from home, or an academy-managed platform.

- Appropriate behaviour is expected at all times, and the academy-managed systems should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the academy into disrepute or compromise the professionalism of staff.

- Staff are allowed to use the email and messaging system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their messages may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to inappropriate sites may be blocked and not arrive at their intended destination.

Academy websites

Academy websites are key public-facing information portals for the academy community (both existing and prospective stakeholders) with a key reputational value. The Headteacher / Principal and Governors have given overall responsibility for the day-to-day updating the content to trusted members of staff. The DfE has determined information which must be available on all school websites.

Where staff submit information for the website, they are asked to remember:

- Academies have the same duty as any person or organisation to respect and uphold copyright law (schools have been fined thousands of pounds for copyright breaches). Sources must always be credited and material only used with permission.

- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (including in file names / metadata).

Cloud platforms

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- New cloud systems and what may or may not be stored in them are approved by the DSL / OSL in consultation with technical staff. This is noted in a DPIA (data-protection impact statement) and parental permission is sought in line with GDPR requirements
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and / or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images / videos are only made public with parental permission
- Only academy-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil / student joins an academy, parents / carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent).

Whenever a photo or video is taken / made, the member of staff taking it will check the latest records of parental consent before using it for any purpose.

Images in public facing materials - such as academy websites and blogs - do not have any name attached. In exceptional circumstances, additional permission from parents may be sought to allow pupils shown in public facing materials to be identified with a first name only.

All staff are governed by their contract of employment and the academy's acceptable use policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. With permission from a member of the senior leadership team, staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to academy activities, taken without secrecy and not in a one-to-one situation, and always moved to academy storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the academy's network in line with the retention schedule of the Data Protection Policy.

Parents are reminded at appropriate times - e.g. before school productions - about the importance of not sharing images taken in school.

Pupils are taught to think about their online reputation and digital footprint, so all staff should be good adult role models by not oversharing.

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.

Pupils are advised to be very careful about placing any personal photos on social media. 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. They are taught about the risks associated with providing information with images (including the name and metadata of the file), that reveals the identity of others and their location. They are taught about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social media

Academies manage and monitor their social media footprint carefully to know what is being said about the academy and to respond to criticism and praise in a fair, responsible manner.

Staff responsible for managing social media accounts follow the guidance in the LGfL / Safer Internet Centre online-reputation management.

Staff, pupils' and parents' social media presence

Social media (including apps, sites and games that allow sharing and interaction between users) is a fact of modern life. However, as stated in the acceptable use policies which all members of the academy community sign, we expect everybody to behave in a positive manner, engaging respectfully with the academy and each other on social media as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the academy or (particularly for staff) the teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the academy, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the Trust's complaints procedure should be followed. Sharing complaints on social media is unhelpful and can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the academy, which is important for the pupils we serve.

Many social media platforms have a minimum age of 13, but the academies deal with issues arising on social media with pupils / students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage underage use.

Academies have to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils / students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will typically learn most from the models of behaviour they see and experience, which will often be from adults. Parents can best support this by talking to their children about the apps, sites and games they use, with whom and for how long.

The academies have official social media accounts and will respond to general enquiries, but asks parents / carers not to use these channels to communicate about their children.

Academy-managed email and messaging are the official electronic communication channels between parents and the academy, and between staff and pupils.

Pupils / students are not allowed to be 'friends' with or make a friend request to any member of staff, governors, volunteers and contractors or otherwise communicate via social media. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the academy.

Staff must not follow public student accounts and pupils / students should not follow staff, governor, volunteer or contractor public accounts. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the Trust or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the academy or its stakeholders on social media and be careful that their personal opinions are not be attributed to the academy, Trust or local authority, bringing the academy into disrepute.

All members of the academy community are reminded that, in the context of social media, it is important to comply with the ELAT policy on Digital Images and Video.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices and bring your own device (BYOD) policy

- **Pupils / students** who carry a mobile phone for their own safety when travelling to and from the academy must place their device in their bag when the bell rings at 8.40am. Students are allowed to remove their phones at the end of the school day. Any device taken anywhere else in the academy without special permission will be confiscated**.** Any attempt to use a phone or other device in the academy without special permission or to take illicit photographs or videos will lead to sanctions.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during academy hours unless there is a professional need to respond to notifications. Devices should not be used for personal reasons during teaching periods without permission from a member of the senior leadership team.

- **Volunteers, contractors, governors** should leave their phones in their pockets. They should not be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission must be sought from a member of staff and the headteacher should be notified. Photos / videos must only be taken in the presence of a member staff.

- **Parents** are asked to leave their phones in their pockets when they are on site. They should ask permission before taking any photos - e.g. of displays in corridors or classrooms - and be reminded of the importance of

not sharing images taken in the academy. Urgent messages to pupils should be sent via the academy office, not to a pupil's mobile phone.

Network / internet access on personal devices

- **Pupils / students** are allowed to connect personal devices to the BYOD network for the purpose of completing school work, only when instructed by staff.
- **Staff** are not allowed access to networked files / drives on personally owned devices, but they are allowed to connect to the BYOD wireless network. Staff may use the Remote Access solution to securely access files.
- **Volunteers, contractors, governors** can, with the headteacher's permission, access a guest wireless network on personally owned devices without access to networked files / drives
- **Parents** are not allowed to connect personal devices to any academy network

Trips / events away from the academies

Teachers on academy trips should only get messages to parents via the relevant academy's office. In very exceptional circumstances, staff using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number using 141.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher / Principal and staff authorised by them have a statutory power to search pupils / property on academy premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material.

Full details of academy search procedures are available in the Trust's Behaviour and Attendance Policy.

Key online-safety staff

The nominated ELAT Safeguarding Trustee is Mr Keith Stewart

Bower Park Academy

- **Principal:** Mr Eddie Aylett
- **Designated Safeguarding Lead / Online-Safety Lead:** Mr Stuart Gander
- **LGC Safeguarding Governor:** Mr Andy Mann
- **Computing Curriculum Lead:** Mr Robert Graham
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Hall Mead School

- **Headteacher**: Mrs Maria Ducker
- **Designated Safeguarding Lead / Online-Safety Lead:** Mrs Nicola Afteni
- **LGC Safeguarding Governor:** Claire Nissen
- **Computing Curriculum Lead:** Mr Kevin Lucas
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

The Brittons Academy

- **Principal:** Mr Will Thompson
- **Designated Safeguarding Lead / Online-Safety Coordinator:** Lauri Cossey
- **LGC Safeguarding Governor:** Elizabeth Dixon
- **Computing Curriculum Lead:** Ms Iyabo Aneke
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Hacton Primary School

- **Headteacher:** Mrs Emily Leslie
- **Designated Safeguarding Lead / Online-Safety Coordinator:** Mrs Emily Leslie
- **LGC Safeguarding Governor:** Mrs Jamie Williams
- **Computing Curriculum Leads:** Mr Jack Martin
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Related documents and references

1. Safeguarding and Child Protection Policy (ELAT)
2. Behaviour and Attendance Policy (ELAT)
3. Anti-Bullying Policy and Procedures (ELAT)
4. Acceptable Use Policies: Pupils; Staff, Volunteers Governors & Contractors; Parents (ELAT)
5. Parental consent forms for photography in school (ELAT)
6. Online-Safety in schools and colleges: Questions from the Governing Board (UKCCIS)
7. Education for a Connected World: A framework to equip children and young people for digital life (UKCCIS / UKCIS)
8. Safer working practice for those working with children & young people in education settings (Safer Recruitment Consortium)
9. Working together to safeguard children (DfE)
10. Searching, screening and confiscation at school (DfE)
11. Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
12. Sexting in schools and colleges: Responding to incidents andsafeguarding young people (UKCCIS)
13. Protecting children from radicalisation: the prevent duty (DfE)
14. New relationships and health education in schools (DfE press release, 19 July 2018)
15. Guide to the General Data Protection Regulation (ICO)
16. Preventing bullying (DfE)
17. Cyberbullying: Advice for headteachers and school staff (DfE)
18. RAG (red-amber-green) audit for statutory requirements of school websites (LGfL)
19. Data Protection: Toolkit for Schools (DfE)