



# The Eliot Bank and Gordonbrock Schools Federation



## Online Safety Policy

<b>Author:</b>	<b>Executive Head</b>	<b>Date:</b>	<b>September 2016</b>
<b>Approved by:</b>	<b>Governing Body</b>	<b>Date:</b>	<b>September 2016</b>
<b>Date of Last Review:</b>	<b>August 2024</b>	<b>Next Review Date:</b>	<b>August 2025</b>

**Contents**

**1. Introduction ..... 3**

**2. Overview ..... 4**

**2.1 Aims ..... 4**

**2.2 Scope ..... 4**

**3. Roles and Responsibilities ..... 5**

**4. Education and Curriculum ..... 6**

**5. Handling Safeguarding Concerns and Incidents ..... 7**

**5.1 Nudes – sharing nudes and semi-nudes ..... 8**

**5.2 Bullying ..... 9**

**5.3 Child-On-Child Sexual Violence and Sexual Harassment ..... 9**

**5.4 Misuse of School Technology (Devices, Systems, Networks or Platforms) ..... 10**

**5.5 Social Media Incidents ..... 10**

**5.6 Extremism ..... 10**

**6. Data Protection and Cyber Security ..... 11**

**7. Appropriate Filtering and Monitoring ..... 12**

**8. Messaging/commenting systems (incl. email, learning platforms & more) ..... 13**

**8.1 Authorised Systems ..... 13**

**8.2 Behaviour / Usage Principles of Messaging / Commenting Systems ..... 14**

**9. Online Storage or Learning Platforms ..... 15**

**10. School Website ..... 16**

**11. Digital Images and Video ..... 17**

**12. Social Media ..... 19**

**12.1 Our SM presence ..... 19**

**12.2 Staff, Pupils’ and Parents’ SM Presence ..... 19**

**13. Device Usage ..... 22**

**13.1 Personal devices including wearable technology and bring your own device (BYOD) ..... 22**

**13.2 Use of School Devices ..... 22**

**13.3 Trips / Events Away from School ..... 23**

**13.4 Searching and Confiscation ..... 23**

## 1. Introduction

### Key People / Dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Jane Wright (Head of School)
Deputy Designated Safeguarding Leads / DSL Team Members	Marinda Barry (Deputy HT) Mark Ridler-Mayor (Deputy HT) Maria Gilmore (Executive HT)
Link governor for safeguarding and web filtering	Peter Fidel (Chair of Governors)
Curriculum leads with relevance to online safeguarding and their role	Tony Hardy-Hall (Technology Team Leader) Anna Gibbons (PSHE Team Leader) Mark Ridler-Mayor (Deputy HT for Curriculum and Assessment)
Network manager / other technical support	Deku Solutions Ltd
Date this policy was reviewed and by whom	August 2024

## 2. Overview

### 2.1 Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Eliot Bank and Gordonbrock Schools Federation community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. Technology, PSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & 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.
- Helping school 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, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

### 2.2 Scope

This policy applies to all members of the Eliot Bank and Gordonbrock Schools community (including teaching, supply and support staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

The following procedure may be engaged at either the informal stage or the formal stage where the employee's capability is of serious concern; including instances where an employee may not accept that a performance problem exists. However, except in the most serious cases, informal action should be taken first. The school's HR adviser in Schools Team Personnel will be able to provide advice as necessary.

### **3. Roles and Responsibilities**

This school 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 school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should read the relevant section in Appendix 1 of this document that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the appendix. All staff have a key role to play in feeding back on potential issues.

#### **4. Education and Curriculum**

Despite the risks associated with being online, Eliot Bank and Gordonbrock Schools Federation recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](#) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

The teaching of online safety, features in these particular areas of curriculum delivery:

- Online safety - National Online Safety (National College)
- PHSE (Personal, Health and Social Education), including RSE (Relationships and Sex Education) - You, Me, PSHE and Christopher Winter Project
- Computing - Teach Computing

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

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access by, for example, publishing this policy and our curriculum on our school website, including online safety tips in our GB Weekly, distribute relevant information from third party organisations and parent workshops.

## **5. Handling Safeguarding Concerns and Incidents**

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support 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.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Preventing Extremism and Radicalisation Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security Policy

This school commits to take all reasonable precautions to safeguard pupils online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on white online safety concern report form - this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

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

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre’s Professionals’ Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance [Behaviour in Schools, advice for headteachers and school staff September 2024](#) provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

The following sub-sections provide detail on managing particular types of concern.

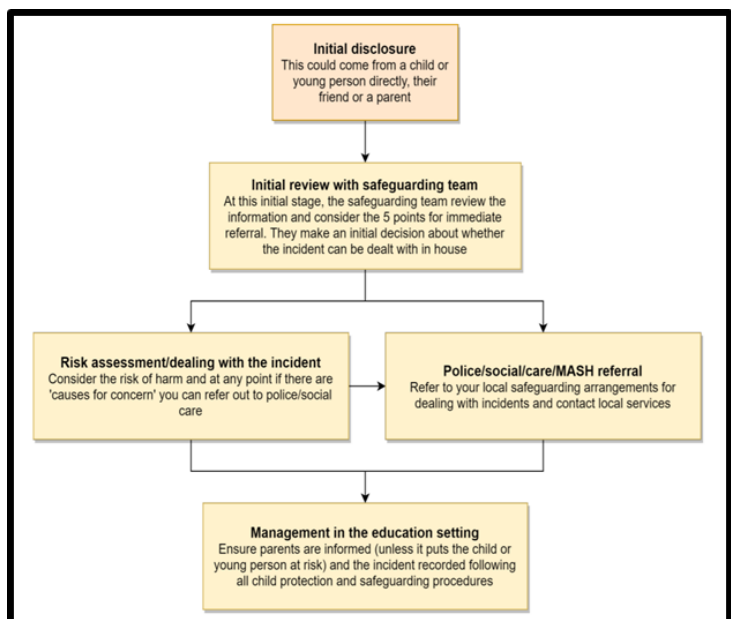
### 5.1 Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#).

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.**

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, pupils should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved (see flow chart on the right from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.





The following LGfL document (available at [nudes.lgfl.net](https://nudes.lgfl.net)) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:


**SAFEGUARDING QUESTION TIME**

**Q: WHEN SHOULD WE REFER NUDE SHARING?**  
**A: IMMEDIATELY \*IF\* THE IMAGE/VIDEO:**

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm[...], suicidal or self-harming

Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS - search.gov.uk

*"We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!"*



**LGfL**  
SafeguardED

### 5.2 Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed. This includes issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at [bullying.lgfl.net](https://bullying.lgfl.net)

### 5.3 Child-On-Child Sexual Violence and Sexual Harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. This will be discussed in staff training.

#### **5.4 Misuse of School Technology (Devices, Systems, Networks or Platforms)**

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy <https://www.gordonbrock.lewisham.sch.uk/policies/> as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy. Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

#### **5.5 Social Media Incidents**

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in the Eliot Bank and Gordonbrock Schools Federation community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), Eliot Bank and Gordonbrock Schools Federation will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

#### **5.6 Extremism**

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty <https://www.gordonbrock.lewisham.sch.uk/policies/>. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

## **6. Data Protection and Cyber Security**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy which can be found here <https://www.gordonbrock.lewisham.sch.uk/policies/> It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

## **7. Appropriate Filtering and Monitoring**

The designated safeguarding lead (DSL) (Jane Wright) has lead responsibility for filtering and monitoring and works closely with Deku to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. They can submit concerns at any point via the white online safety concern report form and will be asked for feedback at the time of the regular checks which will now take place.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out weekly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

SafeSearch is enforced on any accessible search engines on all devices.

Our YouTube mode is set to Strict Restricted Mode for all users.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

The DSL checks filtering reports and notifications monthly and takes any necessary action as a result.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At Eliot Bank and Gordonbrock Schools Federation, we use LGFL's HomeProtect for pupil device loaned for home use.

## **8. Messaging/commenting systems (incl. email, learning platforms & more)**

### **8.1 Authorised Systems**

- Pupils at this school may communicate with staff using Google Classroom via the submit assignment function. Staff may provide feedback following this interaction. There may also be occasions when pupils write a response to staff and pupil messages via the class stream. Although, by default, the class stream is deactivated as it requires regular monitoring by teachers.
- Staff at this school use the email system provided by LGFL for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. When contacting parents via email, staff will liaise with a member of the office team and use info@ or, for more sensitive communications, admin@.
- Staff at this school also use ScholarPack to communicate with parents/carers via email and text.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use 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).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Head of School/Executive Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

## **8.2 Behaviour / Usage Principles of Messaging / Commenting Systems**

- More detail for all the points below are given in the Social media section of this policy as well as the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system 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 school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

## **9. Online Storage or Learning Platforms**

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. In Eliot Bank and Gordonbrock Schools Federation this includes Google Drive.

For all these, it is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it. Any new platforms will be approved by the DHT for Curriculum and Assessment in consultation with the Technology Team Leader and Deku Solutions Ltd.

## **10. School Website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Head of School/Executive Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Anne-Marie Kucukkaramuklu and Mark Ridler-Mayor.

The website is managed by / hosted by LGFL.

Where staff submit information for the website, they are asked to remember that schools 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. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with Anne-Marie Kucukkaramuklu.



## **11. Digital Images and Video**

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- School publications e.g. weekly newsletter, school prospectus, the school website and school's Twitter account.
- Videos for the purpose of promoting the school, such as the school website and school's Twitter account.
- Audio clips for the purpose of promoting the school, such as the school website and school's Twitter account.
- Professional whole-class photos taken by a third-party company. These photos are sold to parents and carers.

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

Any pupils shown in public facing materials are never identified by their name unless permission has been expressly sought from the parent/carer (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Eliot Bank and Gordonbrock Schools Federation, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on local networks in line with the retention schedule of the school Data Protection Policy. Any concerns about the nature of these images will be reported to the DSL.

Staff and parents are routinely reminded about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

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. 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. 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 / or a friend are subject to bullying or abuse.

## 12. Social Media

### 12.1 Our SM presence

Eliot Bank and Gordonbrock Schools Federation works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk)) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Eliot Bank and Gordonbrock Schools Federation is responsible for managing school accounts on X (formerly Twitter) and checking our Wikipedia and Google reviews and other mentions online.

Twitter accounts include:

Eliot Bank	Gordonbrock
@eliotbank	@GordonbrockS @TheArtsatGB

### 12.2 Staff, Pupils' and Parents' SM Presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way 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 school or (particularly for staff) 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 school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 but the school regularly deals with issues arising on social media involving pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has 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 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 often 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 (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the [Digital Family Agreement](#) to help establish shared expectations and the [Top Tips for Parents](#) poster along with relevant items and support available from [parentsafe.lgfl.net](https://parentsafe.lgfl.net) and introduce the [Children's Commission Digital 5 A Day](#).

Although the school has an official X (Twitter) account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children. Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

As outlined in the Acceptable Use Policies, pupils are not allowed<sup>1</sup> to be 'friends' with or make a friend request<sup>2</sup> to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

Staff are reminded that they are obliged not to bring the school 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 school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

---

<sup>1</sup> *Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head of School/Executive Headteacher and should be declared upon entry of the pupil or staff member to the school).*

<sup>2</sup> *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).*

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

### 13. Device Usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

#### 13.1 Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils** (in Year 5 and 6) are allowed to bring mobile phones in as part of safety planning for their journey to and from school. During the school day, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Our approach to pupils using mobile phones is in line with DfE, [Mobile Phone Guidance](#).
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cyber security policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they 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 of the Head of School/Executive Headteacher should be sought (they may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to refrain from using their mobile phones while in the presence of pupils (for example, Open Morning, Parent Events, etc.) They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. A member of staff will remind parents that photos and videos taken at these events are for personal use only and must not be shared online or on social media. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- Staff nor pupils are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

#### 13.2 Use of School Devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy or staff code of conduct.

Wi-Fi is accessible to guests through the guest network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or pupils are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

### **13.3 Trips / Events Away from School**

For school trips/events away from school, teachers will be issued a school mobile phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Head of School/Executive Headteacher. Teachers 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.

If on trips pupils are encouraged to connect to another organisation's Wi-Fi network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school and therefore staff are responsible for risk assessing and managing such situations. Staff should seek advice from the DSL where necessary.

### **13.4 Searching and Confiscation**

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Head of School/Executive Headteacher and staff authorised by them have a statutory power to search pupils/property on school 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, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy <https://www.gordonbrock.lewisham.sch.uk/policies/>.

## **Appendices**

Appendix 1

Online Safety Roles