Emanuel School

Online Safety Policy

1. Introduction

Being online is an integral part of children's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form part of children's online world. The internet and online technology provide new opportunities for young people's learning and growth, but it can also expose them to new types of risks.

Online safety forms a fundamental part of Emanuel School's safeguarding and child protection measures. The school understands its responsibility when it comes to online safety:

- to ensure the school's online procedures keep pupils safe, and
- to educate pupils on online safety issues, to teach them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety.

Working in partnership with pupils, their parents, carers and other agencies is essential in promoting young people's welfare and in helping them to be responsible in their approach to online safety. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

1.1 Purpose

This policy, supported by various school policies including the *Safeguarding and Child Protection Policy*, *Pupil Acceptable Use Agreement* and *Laptop and Mobile Device Policy*, is implemented to protect the interests and safety of the whole school community.

The purpose of this policy is to:

- ensure the safety and wellbeing of pupils when adults or pupils are using the internet, social media or mobile devices.
- set out expectations for all school community members' online behaviour, attitudes and activities and use of digital technology, in and outside school.
- ensure that the school operates in line with their values and within the law in terms of how online devices are used.
- facilitate the safe, responsible, respectful and positive use of technology to support teaching and learning, increase attainment and prepare pupils for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- foster an open environment in which pupils are encouraged to ask any questions and participate in an ongoing conversation about the benefits and dangers of the online world.
- create an environment that maximises the likelihood that children inform a trusted adult if they feel vulnerable or uncomfortable about online interactions or content.
- help 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 pupils 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.
- establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

1.2 Scope

This policy applies to all members of Emanuel School's community including staff, pupils, parents and visitors who have access to and are users of the school's digital systems, both in and out of the school.

This policy covers both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment) as well as devices owned by pupils, staff or visitors and brought onto school premises.

1.3 Classification of Online Risks

The breadth of online safety risks can be classified into four key areas as defined in the DfE guidance *Keeping Children Safe in Education:*

Content	being exposed to illegal, inappropriate or harmful content (e.g. pornography, racist or radical and extremist views, suicide, radicalisation).
Contact	being subjected to harmful online interaction with other users (e.g. online grooming incl. sexual exploitation, radicalisation, extremism, personal data exploitation and misuse).
Conduct	personal online behaviour that increases the likelihood of, or causes harm (e.g. sending and receiving explicit images, or online bullying).
Commerce	risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils may use mobile technology to access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's *Behaviour Policy*.

2. *Roles and Responsibilities*

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as they become apparent.

While this will be a team effort, the following section outlines the online safety roles and responsibilities of individuals and groups within the school.

2.1 Headmaster and Deputy Heads

The headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding. Together with the deputy heads, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

2.2 Designated Safeguarding Lead/Deputy Designated Safeguarding Leads

The designated safeguarding lead takes lead responsibility for day-to-day safeguarding and child protection. This includes responsibility for online safety and understanding of the school's filtering and monitoring systems and processes.

Key responsibilities include but are not limited to:

- be aware of the potential for serious safeguarding issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying,

- work closely with the headmaster and the IT department to ensure that the school's requirements for filtering and monitoring are met and enforced,
- to review filtering and monitoring reports and ensure that termly checks are made of the system,
- to review and drive the rationale behind decisions in filtering and monitoring as per DfE *Meeting Digital and Technology Standards* through regular liaison with IT staff.
- ensure an effective whole school approach to online safety that empowers to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate,
- ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures,
- liaise with the headmaster and Chair of Governors to ensure that all governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated,
- be mindful of using appropriate language and terminology around children when managing concerns, including victim-blaming language,
- remind staff of safeguarding considerations as part of remote learning procedures and technology,
- work with headmaster, bursar/compliance manager 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,
- keep up to date on current online safety issues and updates in online safeguarding and legislation,
- review and update this policy and other online safety documents,
- ensure that online safety education is embedded across the curriculum and beyond,
- promote an awareness of and commitment to online safety throughout the school community,
- ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident,
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments,
- meet regularly with the responsible governor to discuss current issues, review (anonymised) incidents and discuss appropriate filtering and monitoring,

2.2 All Staff

The key responsibilities are:

- to read and follow this policy in conjunction with the school's main *Safeguarding and Child Protection Policy* and the relevant parts of the statutory DfE guidance *Keeping Children Safe in Education*.
- to understand that online safety is a core part of safeguarding and everyone's responsibility.
- to record online safety incidents/concerns in the same way as other safeguarding incidents/concerns.
- to be aware of the emphasis of appropriate filtering and monitoring and to play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking.
- to read and adhere to the *Staff Code of Conduct/Acceptable Use Agreement.*
- to identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE/Life Education curriculum, both outside the classroom and within the curriculum, supporting subject leads, and making the most oof unexpected learning opportunities as they arise.
- to carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- to encourage and talk about appropriate online behaviour, how to get help and consider potential risks.

- to follow best practice pedagogy for online safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- to be aware of security best practice at all times, including password hygiene and phishing strategies.
- to prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- to encourage pupils to follow the *Pupil Acceptable Use Policy* at home as well as at school, remind them about it and enforce school sanctions in line with the *Behaviour Policy.*
- to take a zero-tolerance approach to all forms of (online) child-on-child abuse, this includes bullying, sexual violence and harassment.
- to be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying, sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/DDSL know.
- to have a healthy curiosity for online safeguarding issues.
- to model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- to be aware of sources of support for online safety issues such as the Professional Online Safety Helpline (POSH), Reporting Harmful Content, CEOP and Internet Watch Foundation (IWF) and know how to report harmful and illegal online content (Please refer to appendix 3 *Guide to Reporting Harmful and Illegal Content Online.)*
- to notify the designated safeguarding lead if this policy does not reflect practice in school and follow escalation procedures if concerns are not promptly acted upon.

2.3 Subject Leads Responsibilities

Life Education subject leads work with the DSL to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme,
- PHSE and RSE programmes,
- a mapped cross-curricular programme,
- assemblies and pastoral programmes.

Computing subject leads oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum and work closely with the Life Education subject leads to avoid overlap but ensure a complementary whole-school approach. The Computing subject lead will also collaborate with technical staff and others responsible for IT use to ensure common and consistent approach in line with acceptable use agreements.

Other subject leads must look for opportunities to embed online safety in their subject and model positive attitudes and approaches to staff and pupils alike. They should ensure that subject specific action plans also have an online safety element.

2.4 Head of IT/Technical Staff

Key responsibilities:

- as listed in the 'All Staff' section, plus:
- collaborate regularly with the designated safeguarding lead (DSL) and deputy heads to help them make key strategic decisions around safeguarding elements of technology,
- help DSL/DDSLs to understand systems, settings and implications,
- support, as required, DSL/DDSLs/deputy heads to carry out an annual online safety audit which includes the review of technology, including filtering and monitoring systems,

- keep up to date with the school's *Online Safety Policy* and technical information to effectively carry out their online safety role and to inform and update others as relevant,
- work closely with the DSL/DDSLs, data protection team and life education subject leads to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice,
- maintain up to date documentation of the school's online security and technical procedures,
- maintaining filtering and monitoring systems, providing filtering and monitoring reports and completing actions following filtering/monitoring concerns or checks to systems,
- report online safety related issues that come to their attention in line with school policy,
- manage the school's systems, network and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls,
- ensure cyber related policies are up to date, easy to follow and practicable,
- monitor the use of the internet and emails, school technology, online platforms and that any misuse/attempted misuse is identified and reported to the DSL/DDSLs,
- attend system specific training to support the effective management of technical monitoring/filtering systems (as required).

2.5 Governing Body

Key responsibilities:

- to undergo safeguarding and child protection training (including online safety) at induction to provide strategic challenge into policy and practice, ensuring this is regularly updated,
- to ensure all staff are adequately trained about safeguarding and child protection (including online safety and filtering/monitoring) at induction and that this is regularly updated,
- to ensure that all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to escalate concerns when identified,
- to review the effectiveness of the school's filtering and monitoring systems, strategies and reporting processes,
- to ensure staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school,
- to ensure an appropriate senior member of staff is appointed to the role of DSL with lead responsibility for child protection and safeguarding (including online safety),
- to ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum,
- to consider a whole school approach to online safety with a clear policy on the use of mobile technology.

This list is not intended to be exhaustive.

2.5 Pupils

Key responsibilities include but are not limited to:

- read, understand and adhere to the *Pupil Acceptable Use Agreement (AUA),*
- understand the importance of reporting abuse, misuse or access to inappropriate materials including any concerns about a member of school staff or supply teacher,
- know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else,
- understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use agreement covers actions out of school, including social media,
- remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher,

- understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.
- take advantage of opportunities for engagement on online safety support offered (including specialised online safety training and resources).

This list is not intended to be exhaustive.

2.6 Parents and Carers

Parents and carers play a crucial role in promoting online safety both within and outside school.The school encourages parents and carers to maintain an open and ongoing discussion about online safety at home/as a family/with their child(ren).

Emanuel School seeks to work closely with parents in promoting a culture of online safety and shares relevant resources via newsletters, email and/or Firefly and invites parents to online safety information sessions.

Parent/carer key responsibilities include, but are not limited to:

- contact their child's form tutor if they have any concerns about their child's and others' use of technology,
- read the *Pupil Acceptable Use Policy* and encourage their child to follow it,
- promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media (e.g. not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others),
- support their child during any home/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 changed where possible.
- talking to their child about the apps, sites and games they use, with whom, for how long, and when.
- respect age ratings on social media platforms wherever possible and not to encourage or condone underage use by their child.

This list is not intended to be exhaustive.

The school will contact parents if it has any concerns about a pupil's behaviour in this area and likewise hopes that parents will feel able to share any online safety concerns with the school.

3. Online Safety Education and Engagement Approaches

3.1 Online Safety Education – Pupils

Whilst regulation and technical solutions are particularly important, their use must be balanced by educating pupils to take a responsible approach. At Emanuel School it is recognised that online safety and broader digital resilience must be thread throughout the curriculum.

The school's Life Education programme and Computing classes teach pupils in an age-appropriate way about online safety, including developing knowledge and behaviours to help pupils navigate the online world safely and confidently and incorporates online safety information on the dangers of cyberbullying and sexting (sharing nudes/semi-nudes) and emphasises the need to build resilience, including to radicalisation, in pupils. This includes navigating the internet and managing information, how to stay safe online and covering elements of online activity that can adversely affect a pupil's wellbeing. Key online safety messages are also delivered in assemblies or form time. External speakers are also regularly invited to supplement and reinforce the school's online safety curriculum and contribute towards pupils' online safety awareness.

As stated in the '***Roles and Responsibilities'*** above, 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 and making the most of unexpected learning opportunities as they arise.

Emanuel School recognises that every child is unique and so is their online experience. Research has shown that children facing offline vulnerabilities are more at risk online and that their offline vulnerabilities inform which types of risk they will encounter online[1].
The school will ensure that differentiated and adapted online safety education, access and support is provided to vulnerable pupils as required to enable them to have a safer online experience and to thrive in the digital world.

Curriculum plans/schemes of work (including for SEND pupils) are reviewed annually. Examples from the school's curriculum include:

Lower School	
Y6	• Well-being and social media. What are the positives and negatives. Other ways to communicate and have fun. Signposting. • Newswise – what to believe and what to question • Internet content and contact (Be SMART online) • Risks of network devices including Firewalls, Anti-virus, Hacking, strong passwords and data protection
Y7	• Cyberbullying: • Digital resilience: • Risks of network devices including Firewalls, Anti-virus, hacking, strong password and data protection
Y8	• Wellbeing and social media: Using social media responsibly and the importance of offline activities: • Online Stress: Online friends v real and FOMO • Sexting • Review of the risks of network devices including Firewalls, Anti-virus, hacking, strong password and data protection

[1] From Survive to Thrive: Supporting Digital Family Life after Lockdown (Internet Matters, Spring 2021)

Middle School	
All pupils in the middle school receive information regarding the schools "Acceptable Use Policy", alongside advice about how you can use the internet safely, responsibly and positively. This includes how to protect your online reputation, know where to find help, don't give in to pressures, respect the law and acknowledge your sources.	
Y9	▪ All pupils in Y9 study an online digital awareness curriculum designed by Digital Awareness UK. The curriculum is designed to encourage critical thinking and self-reflection. The course uses AI and is delivered in year 9 in partnership with the Life Education and assembly programme. The modules tackle some of the most challenging topics in the online safety and digital wellbeing space as well as the unique challenges that come with using technology. Modules covered; Posture wellness, Balance & Screens, Scams, Sexting & consent, Sleep and Screens, Trash Talk & In-Game Abuse, Hacking, Digital Eye Strain, Online Hate Speech and The Digital Footprint. ▪ Pupils will also have an external talk from the Metropolitan Police on their Cyber Choices programme and a talk from Natasha Devon.
Y10	▪ Pornography – the law and revenge porn ▪ Consent and sexual violence – their rights and how to keep safe and healthy in relationships.
Y11	▪ Managing unwanted attention ▪ All pupils in Year 11 complete an online digital course exploring mental health using the Wellbeing Hub.
Sixth Form	
Y12	▪ Pornography and the brain – neuroplasticity and sexting ▪ Pornography – the law and revenge porn ▪ Raising awareness of one's digital footprint, and the risks associated with one's online profile
Y13	▪ Understanding how social media influences body image (RAP Project) ▪ Consent and sexual violence – rights and how to keep safe and healthy in relationships ▪ Understanding rape culture and managing unwanted attention/sexual harassment

3.2 Online Safety Awareness & Training – Staff

All new members of staff receive information on the school's *Online Safety Policy* and *Code of Conduct* as part of their induction programme.

Staff will be provided with up-to-date and appropriate online safety training on a regular basis with at least annual updates. Teaching staff receive information about online safety issues at staff meetings as and when required.

Sources of support can be found in Appendix 2.

3.3 Online Safety Awareness & Training – Parents/Carers

Parents/carers have the opportunity to engage in our rolling programme of online safety advice, guidance and training. The school welcomes parent/carer views on the topics which they would like support on.

Sources of support can be found in Appendix 2.

4. Responding to Online Safety Incidents/Concerns/Disclosures

Internal school channels should always be followed first for reporting and support, especially in response to incidents, which should be reported in line with the school's *Safeguarding and Child*

Protection Policy. All members of the school community are encouraged to be vigilant in reporting online safety concerns/incidents in the confidence that issues will be dealt with quickly and sensitively.

Support strategies are in place for those reporting or affected by an online safety incident. Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.

The school will actively seek support from other agencies as required (e.g. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NSPCC Report Abuse Helpline, NCA CEOP, Police, IWF and Harmful Sexual Behaviour Support Service).

4.1 Responding to Online Safety Incidents Involving Pupils

If a pupil feels uncomfortable or worried by anything online or on a device, they are encouraged to tell a trusted adult as soon as possible. Pupils can also use the button on Firefly to report any pastoral (including online) concerns.

4.1.1 Responding to Online Abuse/Child-on-Child Abuse Disclosure

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices. It can happen anywhere online that allows digital communication (e.g. in messaging apps, online chats, voice chat in games, comments on live streaming sites) and may include cyberbullying, emotional abuse, sexting, sexual abuse/exploitation/harassment and grooming. The school will respond to concerns and disclosures regarding child-on-child (online) abuse regardless of whether the incident took place in school or out of school, using school or non-school devices.

Staff members have the understanding that a pupil may be reluctant to speak out about abuse they have experienced online. Every disclosure will be taken seriously and staff will always make the pupil feel supported and not feel ashamed or given the impression that they are causing problems.

When responding to cases of online abuse, the school will consider the impact it can have on the pupil's wellbeing and provide the child with the right counselling/pastoral support.

<u>If it is believed that the pupil is in immediate danger, the police need to be contacted on 999.</u>

If the pupil is not in immediate danger, the DSL/DDSL must be informed of any online safety concerns and the school's child protection procedures will be followed in line with the school's *Safeguarding and Child Protection Policy*.

Parents/carers will be informed about cases of online abuse unless to do so would put a child at further risk of harm.

4.1.2 Incident of Pupil Misuse

Any allegation, concern or suspicion that a pupil has been involved in any of the following should be reported immediately to the deputy head: pupils/designated safeguarding lead and action will be taken in accordance with the school's *Safeguarding and Child Protection Policy, Searching and Confiscation Policy, Behaviour Policy* and *Anti-Bullying Policy*:

- possession of, or access/attempted access to a website containing images of child abuse,
- possession of, or access/attempted access to a website containing illegal *(e.g. obscene or criminally racist)* or terrorist or extremist material,
- any incident by electronic means involving 'grooming' behaviour,
- any other incident *(which may include instances of upskirting or sharing of nudes/semi-nudes)* that suggests that a pupil or another child has suffered or is at risk of suffering serious harm.

Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft, unlicensed use of software or unlawful use of personal data should be reported to the deputy

head: pupils/designated safeguarding lead. Such concerns will be managed in accordance with the school's *Behaviour Policy* although referrals may be made to outside agencies as appropriate.

4.1.2.1 Responding to Nudes/Semi-Nudes Incidents (Sexting)

It is important to remember that the production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Staff should **immediately** report any incident to the designated safeguarding lead and follow the below UKCIS *Sharing Nudes and Semi-Nudes: How to Respond to an Incident* (Appendix 1):

- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.[1]
- If you have already viewed the imagery by accident (e.g. if someone has shown it to you before you could stop them), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

[1] In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).

Staff should also refer to the *Searching and Confiscation Policy*.

The sharing of nudes or semi-nudes may constitute a criminal offence and will be considered in accordance with the school's *Safeguarding and Child Protection Policy* and advice published by the UK Council for Child Internet Safety: '*Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People*'. The DSL will decide next steps and whether other agencies need to be involved.

Incidents involving the sharing of nudes and semi-nudes will be recorded on the school's online incident log.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

4.1.2.2 Upskirting Incident

Upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in *Keeping Children Safe in Education.*

4.1.2.3 Cyberbullying Incident

Any allegation of cyberbullying should be reported to the deputy head: pupils/designated safeguarding lead as soon as possible. Cyberbullying incidents, including incidents that take place outside school or from home, will be dealt with in accordance with the school's *Anti-Bullying Policy* and *Behaviour Policy*.

Any other misuse of the school's IT facilities not falling within one of the categories above should be referred to the deputy head: pupils/designated safeguarding lead who will take action as appropriate in accordance with the school's *Behaviour Policy* and *Pupil Acceptable Use Policy*.

4.2 Procedures for Dealing with Online Safety Incidents Involving Staff

Any allegation, complaint, concern or suspicion that a member of staff has been involved in any of the following should be reported immediately to the designated safeguarding lead and the headmaster *(or to the chair of governors and the LADO if the headmaster is the subject of the concern):*

- possession of, or access/attempted access to websites containing images of child abuse,
- possession of, or access/attempted access to a website containing, illegal *(e.g. obscene or criminally racist)* or terrorist or extremist material,
- any incident by electronic means involving 'grooming' behaviour,
- any other incident *(e.g. sharing of nudes/semi-nudes)* that suggests that a pupil or another child has suffered or is at risk of suffering serious harm from a member of staff.

Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft or unlawful use of personal data should be reported in line with the school's *Whistleblowing Policy*.

Any other unsuitable activity or access to unsuitable materials should be reported to the designated safeguarding lead who will act as appropriate in accordance with the school's disciplinary procedures. Please also refer to the *Neutral Notification Guidance*.

Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

4.3 Social Media Incidents

Social media incidents are governed by the school's acceptable use policies and breaches will be dealt with in line with the *Behaviour Policy* (for pupils) or the *Disciplinary Procedure* (for Staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school 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 external helplines for support or help to accelerate this process.

4.4 Filtering and Monitoring Incidents

Any report of filtering and monitoring incidents will be reviewed by the deputy head: pupils / designated safeguarding lead. Where the incident requires further action or follow up, they will lead this themselves or delegate to the appropriate member of the pastoral team. A log will be kept of all significant filtering and monitoring incidents.

5 IT Infrastructure Management

5.1 Technical Security and Data Protection

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Emanuel School manages data in compliance with the Data Protection Act 2018 and as outlined in the *Data Protection Policy*.

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements. This includes but is not limited to:

- regular reviews and audits of the safety and security of the school's technical systems. This may periodically be supplemented by an external audit and review.
- servers, wireless systems, and cabling are securely located and physical access restricted,
- rigorous and verified back-up routines,
- clearly defined access rights for all users to school technical systems and devices,
- protection of all school networks and systems by secure passwords,
- ensuring that all software purchased and used by the school is adequately licenced and that the latest software updates are applied.

In addition, the school

- has appropriate security measures in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data,
- has installed up-to-date endpoint (anti-virus) software to protect the school infrastructure/individual workstations,
- uses a recognised internet service provider,
- actively monitors and filters any inappropriate websites or content *(see 'Appropriate Filtering/Monitoring' 5.2/5.3),*
- uses an encrypted and password protected Wi-Fi network.

The *Data Protection Guidelines for Staff* advises staff on best practice to keep information secure and staff should ensure they take appropriate security measures to prevent unlawful or unauthorised processing of the personal data and against the accidental loss of personal data.

5.2 Effective Filtering and Monitoring

The school works closely with governors in all aspects of filtering and monitoring. Filtering and monitoring policies are reviewed at least annually and updated by the DSL and the head of IT to identify gaps in the current provision and the specific needs of pupils and staff. The DfE guidance *Meeting Digital and Technology Standards for Schools/Colleges* is followed.

5.2.1 Effective Filtering

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering".*

- The school manages access to content across its systems for all users and on all devices using a filtering system that meets the standard defined in UKSIC Appropriate Filtering for Education Settings (May 2023) and which blocks illegal content (e.g. websites containing illegal, pornographic, violent, abusive, terrorist or extremist material or that promote the illegal use of drugs or substances). Social networking sites, as well as gaming and other similar sites will be blocked.
  In line with the statutory DfE guidance *Keeping Children Safe in Education*, the school is mindful that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective and that it needs to be supported with good teaching and learning practice and effective supervision.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the designated safeguarding lead to breaches, which are then acted upon.

5.3 Effective Monitoring

Monitoring user activity is an important part of providing a safe environment for children and staff. The school takes advice from the guidance UKSIC *Appropriate Monitoring for Schools (May 2023)* and

DfE *Meeting Digital and Technology Standards for Schools/Colleges* and has effective monitoring systems in place to protect the school, systems and users.

Third-party assisted monitoring software is installed on school issued devices. Technical monitoring is complimented by effective supervision in the classroom. Logs of technical monitoring are reviewed by IT staff and any issues reported to the designated safeguarding lead.

The designated safeguarding lead takes lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. There are effective protocols in place to report abuse/misuse and for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts are in line with the school's *Safeguarding and Child Protection Policy*.

The school monitors network use across all devices and services. The school would only access, monitor and control an individual user's data in response to specific circumstances which might imply possible misuse and following specific authorisation from either the deputy head: pupils/designated safeguarding lead or bursar.

5.4 Mobile Technology

All use of the school network, of personal devices in school and of devices owned by the school *(whether on or off the school site)* must comply with the *Laptop and Mobile Device Policy* and acceptable use policies/agreements. Failure to comply with the policy may result in disciplinary sanctions for pupils in accordance with the school's *Behaviour Policy* and for staff under the school's *Disciplinary Procedure.*

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety programme.

6 Safe Use of Digital Tools/Communications Tools

6.1 Use of Digital and Video Images

Staff, parents/carers and pupils need to be aware of the risk associated with publishing digital images on the internet. Such images may provide avenues for online bullying/cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Staff should inform and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images and encourage pupils to think about their online reputation and digital footprint.

When a child joins the school, parents are asked to complete the *Photographic Image and Video Consent Form* with their child. Staff should only use images of children where permission has been obtained, and only for the given purpose.

Photographs published on the school website/on social media platforms must be selected carefully and must never identify pupils by full name. The school does not use pupil's names when saving images, in the file names/tags. Pupils, staff and parents should refer to the *Photographic Image and Video Policy* for further information.

Staff and parents are reminded about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

6.2 Social Media

All members of the school community are expected to engage in social media in a positive, safe and responsible manner and to be mindful when publishing thoughts, concerns, pictures and messages.

Social media may be used as a beneficial resource for example to enhance engagement in the classroom, celebrate pupil's work, or circulate news and events to parents. The school will always consider the safety implications when using social media with pupils.

If a member of staff considers the use of social media accounts for educational purposes, a proposal must be submitted to the designated safeguarding lead and head of IT, and authorisation received in advance. The use of social media within school will only be permitted in appropriately controlled situations.

6.2.1 Personal Use of Social Media – Staff

The safe and professional use of social media is described in the school's *Staff Code of Conduct*. Staff must not access social media sites for personal use via school systems or using school devices. All members of staff

- are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Disciplinary action may be taken if staff are found to bring the profession or school into disrepute.
- are advised to safeguard themselves and their privacy when using social media sites.
- are encouraged to carefully consider the information (including text and images) they share and post online.
- are aware that information and content that they have access to as part of their employment will not be shared and discussed on social media sites.
- will notify the designated safeguarding lead (DSL) immediately if they consider that any content shared on social media conflicts with their role (Neutral Notification).
- are advised not to communicate with or add as 'friends' any pupils or their family members; exceptions might apply *(e.g. pre-existing contacts)*. Any communication from pupils and parents/carers received via their personal social media accounts should be reported to the DSL.

This list is not intended to be exhaustive.

6.2.2 Personal Use of Social Media – Pupil

Many social media platforms have a minimum age of 13. The school asks parents/cares to not encourage or condone underage social media site use by their child.

Safe and appropriate use of social media will be taught as part of an embedded and progressive education approach. The online safety education also includes online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse.

The filtering system on the school's network is designed to block access to social media sites for pupils.

Pupils are advised:

- to use social media sites which are appropriate for their age and abilities,
- to consider the benefits and risks of sharing personal details (including personal photos) on social media sites which could identify them and/or their location,
- to only approve and invite known friends on social media sites and to deny access to others by keeping online profiles private,
- to not post or send images or videos of others without their permission,
- to use safe passwords,

- to block and report unwanted communications,
- to report concerns – both within school and externally,
- to not send 'friend requests' to any member of staff, governors, volunteers and contractors or to otherwise communicate with them via social media,
- to not 'follow' staff, governor, volunteer or contractor public accounts.

Any concerns regarding a pupil's use of social media will be dealt with in accordance with the school's *Safeguarding and Child Protection Policy*. Concerns will be shared with parents/carers as appropriate.

6.2.3 The School's Social Media Presence

The school manages and monitors their 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.

6.3 Communication Systems (incl. Email, Learning Platforms)

Pupils and staff may only use communication systems that are centrally managed and administered by the school. 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.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the designated safeguarding lead (if by a child) or to the headmaster and designated safeguarding lead (if by a staff member).

7. Policy Review and Approval

Technology and the online environment are constantly changing. The school's *Online Safety Policy* will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.

Policy Owner	Deputy Head: Pupils/Designated Safeguarding Lead
Date of last review	August 2023
Approved by	Cabinet: 21 November 2023
Governor Committee	Pastoral: 24 January 2024
Date of next review	Summer 2024

Table of Changes

Date	Change
March 2024 (V3)	Updated reference to UKCIS guidance *Sharing Nudes and Semi-Nudes: Advice for Education Settings* (March 2024) including Appendix 1 update.

8. Related Policies and Documents

- Anti-Bullying Policy
- Behaviour Policy
- Data Protection Policy
- DfE Keeping Children Safe in Education
- DfE Meeting Digital and Technology Standards in Schools and Colleges
- DfE Teaching Online Safety in Schools
- Information Security Policy
- Laptop and Mobile Device Policy
- Life Education Policy
- NSPCC Protecting Children from Online Abuse
- Photographic Image and Video Policy
- Pupil Acceptable Use Policy

- Remote Education Policy
- Safeguarding and Child Protection Policy
- Searching and Confiscation Policy
- Staff Code of Conduct
- UKCIS Using External Expertise to Enhance Online Safety Education (September 2022)
- UKCIS Sharing Nudes and Semi Nudes: Advice for Education Settings Working with Children and Young People | Full Guidance (March 2024)
- UKCIS Sharing Nudes and Semi-Nudes: How to Respond to an Incident | Overview (2024)
- UKSIC Appropriate Filtering for Education Settings (May 2023)
- UKSIC Appropriate Monitoring for Schools (May 2023)

Appendix 1: Sharing Nudes and Semi-Nudes: How to Respond to an Incident

The below guidance is intended for staff. The designated safeguarding lead/deputy designated safeguarding lead will refer to the full UKCIS guidance.

Sharing nudes and semi-nudes: how to respond to an incident

An overview for all staff working in education settings in England

UK Council for Internet Safety

This document provides a brief overview for frontline staff of how to respond to incidents where nudes and semi-nudes have been shared.

All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) or equivalent and managed in line with your setting's child protection policies.

The DSL or equivalent should refer to the full 2024 guidance from the UK Council for Internet Safety (UKCIS), **Sharing nudes and semi-nudes: advice for education settings working with children and young people**, for managing incidents.

What do we mean by sharing nudes and semi-nudes?

In the latest advice for education settings (UKCIS, 2024), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. Nudes and semi-nudes can be shared online via social media, gaming platforms, chat apps, forums, or involve sharing between devices using offline services. Alternative terms used by children and young people may include 'dick pics' or 'pics'. The motivations for taking and sharing nude and semi-nudes are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. **Your setting's child protection policy should outline codes of practice to be followed.**

- **Never** view, copy, print, share, store or save the imagery yourself**,** or ask a child to share or download – **this is illegal**.[1]
- If you have already viewed the imagery by accident (e.g. if someone has shown it to you before you could stop them), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

[1] In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).

Appendix 2: Sources of Online Safety Support and Teaching Resources

- CEOP – Education Programme (ThinkUKnow)
- CEOP – Safety Centre
- Childnet – Help/Advice and Resources for Teachers and Professionals
- Childnet – Help/Advice and Resources for Parents/Carers
- Common Sense Media
- Education for a Connected World
- Internet Matters – Online Safety Teaching Resources
- Internet Watch Foundation (IWF)
- LGfL – Online Safety Resources
- NSPCC – Keeping Children Safe Online
- NSPCC Report Abuse Helpline
- ProjectEVOLVE
- Report Harmful Content | Advice
- SWGfL – Interface | Online Safety Podcast Series | General Online Safety Resources
- UK Council for Internet Safety (UKCIS)
- UK Safer Internet Centre (UKSIC) – Guides and Resources for Teachers and School Staff
- UK Safer Internet centre (UKSIC) – Guides and Resources for Parents and Carers

Appendix 3: Guide to Reporting Harmful and Illegal Content Online

Detailed guidance on online reporting can be found here.