Freemen's

Learn, lead and make a difference

CITY OF LONDON FREEMEN'S SCHOOL

Online Safety Policy

for both the Junior School and Senior School

Version number	2.0
Name and appointment of owner / author	Stuart Bachelor, Deputy Head and Designated Safeguarding Lead
Review Body	Safeguarding Team, SLT, Finance, General Purposes & Estates Committee and Full Board of Governors
Last updated	17th October, 2021
Reason for update	biennial review
Last reviewed by SLT	October 2021
Last reviewed by Governors	November 2019 (Full Board)
Next Safeguarding Team review due	June 2023
Next SLT review due	September 2023
Next Governor review due	October 2021 (FGP&E Committee)
Where available	Freemen's Staff SharePoint site, Parent Portal, Governor Portal

Online Safety Policy

Authority and circulation

1. This policy has been authorised by the Governing Body of the City of London Freemen's School. It is addressed to parents and pupils and to all members of the teaching and administration staff. This policy is available on a restricted area of the School's website.

Policy Statement

2. Modern young people spend much time online, both at school and elsewhere, and the internet provides and facilitates an unparalleled number and range of opportunities for personal development, social interaction and education. However, as with all activities undertaken by children, their safety online is paramount, and this Policy seeks to outline steps taken by Freemen's to reduce and control risks associated with the internet and electronic communications.

3. The Government's lead guidance on safeguarding in schools, *Keeping Children Safe in Education* (2021), identifies ~~three~~ four main types of online risk faced by children:

• **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and financial scams.

These three risk-types are addressed in this Policy.

4. **Review.** This Policy is reviewed annually by the Safeguarding Team, all of whom have a Designated Safeguarding Lead level of training, and biennially by SLT and Governors.

5. **Compliance.** This Policy should be read in conjunction with the following School documents:

Anti-bullying Policy
Behaviour Policy
Boarding A-Z
Boarding Policy
Boarding Staff Handbook
Computer Network Acceptable Use Policy for Pupils (Junior School version)
Computer Network Acceptable Use Policy for Pupils (Senior School version)

Safeguarding Policy
Searches and Confiscation Policy
Staff Code of Conduct (appended to *Safeguarding Policy*)
Staff Social Media and Photography Guidelines

and the following City of London documents:

Acceptable Use of IT Policy- E-mail and Social Media
Acceptable Use of IT Policy- Internet Access Statement

Key personnel

6. In line with *Keeping Children Safe in Education* (2021), Stuart Bachelor, in his role as Designated Safeguarding Lead, takes ~~lead~~ overall responsibility for online safety.

   The Assistant Head of Upper School, currently Kathryn de Villiers, has the role of Online Safety Co-ordinator. Her work is overseen by the Designated Safeguarding Lead. She is trained as a Deputy Designated Safeguarding Lead.

   The Safeguarding Team, which comprises the DSL and nine Deputy Designated Safeguarding Leads, meets half-termly to discuss both the operational and strategic aspects of safeguarding, including online safety.

   Adam Cohen, Infrastructure and Projects Manager, takes a technical lead on internet monitoring and filtering.

Responding to online safety concerns

7. ~~A flowchart supporting staff in how to respond to online safety concerns can be found at Appendix 7 of our *Safeguarding Policy*.~~ The main thing for staff to note is that an online safety concern should be treated the same as any other safeguarding concern. The following is a selection of types of concerns about children's online behaviour that should be treated as a safeguarding concern:

   Content
   - access to online pornography deliberately facilitated by an adult or through an unequal relationship with another child;
   - accessing online pornography under the age of 13;
   - accessing exploitative or violent pornography;
   - exposure to age-inappropriate violence, horror or gore;
   - any engagement with or interest in racist or extremist online propaganda;

   Contact

Commented [SB1]: This flowchart has been removed from Surrey's template safeguarding policy and has, therefore, also been removed from ours.

- developing a close relationship with someone online without really knowing who he/she is;
- developing an online relationship predicated on secrecy;
- arranging to meet an online friend alone for the first time;
- being approached by an adult-age stranger online;
- being approached online in an unofficial capacity by someone in a position of trust;
- joining adult-only social networking or dating sites;
- giving out contact details online;
- moving away from a public forum to spend time in 'private' chatrooms;
- using social media forums that permit un-attributable posts deliberately to facilitate slander, defamation and cyberbullying;
- receiving requests to produce / send sexual imagery;
- being targeted by commercial advertising for age-restricted products and services such as gambling or sexual services;
- is afraid to use, or obsessively checks, social media and mobile phone messages;

Conduct

- using the internet to bully others, especially if done so anonymously or using an app designed to expunge any evidence;
- cultivating an older online persona;
- receiving nudes / semi-nudes and not deleting them immediately;
- creating nudes;
- disseminating nudes without consent;
- soliciting nudes.

Commerce

- gambling online;
- being exposed to inappropriate advertising, such as for sex products, sexual services, pornography or age-inappropriate video games;
- being targeted by phishing or other financial scams.

Staff are aware that the School's *Searches and Confiscation Policy* empowers them to search and confiscate pupils' electronic devices if there is a good reason to do so.

Nudes and semi-nudes (Youth-produced sexual imagery ~~(YPSI~~)

8. The School takes ~~YPSI~~ nudes and semi-nudes extremely seriously, recognising that it is against the law and places the young people involved at risk of harm. Full details of the School's procedures regarding ~~YPSI~~ nudes can be found in Section 26 of our *Safeguarding Policy*; applicable sanctions are detailed in our *Behaviour Policy*

Cyberbullying

9. It is a sad reality that the online environment can be used to to increase the impact of bullying behaviour upon victims. This is for several reasons:

a. some social media sites and messaging platforms allow comments to remain unattributable;
b. apps such as Snapchat auto-delete posts, making it harder to gather evidence of bullying;
c. hyperconnectivity means that victims may feel that they simply cannot escape a bully;
d. because of FOMO ("fear of missing out"), victims may continue to use a platform despite knowing that it may be used to target them;
e. bullying by exclusion can be made easy by, for instance, simply posting images of a party to which someone was deliberately not invited;
f. the online 'space' is, in contrast to corridors and classrooms etc., largely unmonitored by adults.

Filtering and monitoring pupil access to the internet

10. As *Keeping Children Safe in Education* makes clear, a school's duty of care to its pupils necessitates blocking access to potentially harmful sites and monitoring pupil use of the School internet- while at the same time not hampering legitimate access to the web at the risk of driving pupils onto an alternative unfiltered and unmonitored network. Therefore:

- we use the Smoothwall suite of products to block pupil access to sites considered potentially dangerous because they promote or contain images of radicalisation, self-harm, intolerance, suicide, pornography, illegal drug use, criminal activity, bullying, violence, eating disorders or personal weapons;
- during school hours we block certain apps and websites considered either inappropriate or a detrimental use of pupil time, including Facebook and Twitter;
- Instagram is blocked for day pupils at all times, and for boarders during school hours;
- Snapchat is blocked for all users;
- sites such as Google and Youtube can be accessed by pupils at all hours, but content is age-restricted;
- selected gaming sites in Walbrook (the boarding house) are permitted outside of school time for a restricted period and must be played in social areas;
- the Safeguarding Team receives a daily report from Smoothwall detailing individual pupils who have tried to access potentially dangerous sites;
- Heads of Sections investigate breaches by day pupils and the Head of Boarding those by boarders, liaising with Adam Cohen to find out more details about the site concerned and/or speaking to pupils to find out whether it was visited deliberately, unwittingly or in the course of legitimate study (e.g. researching the topic of illegal drugs for PSHE or an Extended Project);
- we invite pupils to request that certain sites be unblocked and encourage School Council Representatives to flag up any recurring issues with over-blocking.

11. Staff use of the School's network is filtered and monitored in the same manner, although IT Services will unblock certain sites on request. Matt Robinson and Stuart Bachelor receive a daily report from Smoothwall listing members of staff who have tried to access potentially

dangerous sites. Normal procedures are followed if this behaviour amounts to a safeguarding concern. Alternatively, the Deputy Head may consider it appropriate to take a disciplinary approach.

Social Media

12. The School's *Staff Code of Conduct* and *Staff Social Media and Photography Guidelines* cover the safeguarding aspects of social media use by staff.

13. Our policy, guidelines and rules for pupil use of social media can be found at Appendix A below.

Pupil personal data and images

14. A pupil is placed at risk if his/her personal information- name, address, date of birth, what he/she looks like etc.- falls into the hands of someone who would do him/her harm. We are also aware that legal and innocent images of children posted online are sometimes downloaded and manipulated by paedophiles in order to create child pornography. Therefore, the School:
    - has a package of security measures designed to protect the Management Information System on which such information is stored, including timing out sessions and insisting on use of a robust passphrase;
    - avoids printing off such data when it can be accessed electronically;
    - only publishes identifiable images of pupils externally if there is parental consent to do so, as well as seeking separate consent for internal publications such as newsletters;
    - does not use identifiable images of pupils from other schools;
    - uses no more than a first name and initial of surname alongside internally and externally published pupil images;
    - prohibits photography of pupils in swimming gear other than by a professional photographer authorised and accompanied by the Marketing Manager- and then only of pupils who are submerged in the water and unidentifiable (hat and/or goggles);
    - prohibits staff from using personal devices to create or store images of pupils.

Use of pupil-owned mobile 'phones and internet-enabled devices

15. *Keeping Children Safe in Education* states: "Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). Schools and colleges should carefully consider how this is managed on their premises and reflect [this] in their mobile and smart technology policy and their child protection policy."

16. Mindful of this obligation, in September 2019, and following a wide consultation and subsequent trial, the School decided to tighten its policy on pupil mobile 'phone use. Pupils below the Sixth Form are not allowed to use their 'phones (or other internet-enabled

devices) during school hours without staff permission. Sixth-Formers may do so during free time, but only in the Sixth Form Centre (Main House) or to listen to music during Private Study in the Library. Pupils in breach of these rules have their 'phones confiscated and returned at 4 p.m., and are issued a Behaviour Warning.

Pupils and their parents are aware that the School's *Behaviour Policy*, including suspension in the most serious cases, will be applied for inappropriate conduct or bullying online.

Pupil use of school computers and other digital devices

17. There are a Senior School and Junior School versions of the *Computer Network Acceptable Use Policy for Pupils*, by which all pupils are expected to abide. A summary of the policy appears on the landing page when pupils use the internet for the first time that day and has to be acknowledged before browsing can commence.

18. For rules governing boarders' use of computers and devices, please see *Boarding A-Z.*

19. With the issuing of school-owned iPads to KS3 and KS4 pupils in September 2021, the School has been mindful of the possibility of pupils using the 'hotspot' facility on their personal 'phones to obtain unfiltered internet access on their new iPads. Accordingly, during lunchtimes and Break iPads may only be used in the Library.

Virtual Private Networks (VPNs)

20. In the context of a school, a VPN is software employed by a pupil to use the school internet connection while circumventing the School's filters and thus concealing his/her browsing activity. VPNs carry a high risk and attract a serious sanction if found to be used (see *Behaviour Policy*).

21. We control this risk by configuring Smoothwall to block commonly known VPN sites. ~~Given that we know that it is mainly boarding pupils who have the motive and opportunity to use VPNs, from time to time we may monitor boarders' use of the network, cognisant that inexplicably low usage by an individual may indicate a VPN~~and by scanning for pupil use of known VPNs. If boarding staff have reasonable suspicion of VPN usage, the School's *Searches and Confiscation Policy* allows for a boarder's room to be searched. Every opportunity is taken to educate pupils and parents about the dangers of VPN use.

22. Experience suggests that VPNs tend to be used by ~~boarders~~ pupils for undesirable rather than nefarious or harmful purposes; indeed, in some cases they are resorted to in order to access sites for entirely legitimate learning purposes. In an effort to minimise VPN use and its attendant safeguarding risks, ~~boarding staff~~we promote a culture of honesty and compromise regarding sites that ~~boarders~~ pupils would like to be unblocked.

Staff use of computers, mobile 'phones and other digital devices

23. New staff are issued with the City's *Acceptable Use of IT Policy* regarding e-mail, social media and the internet, and are asked to sign to acknowledge that they have read and understood it. The same is the case for the *Staff Code of Conduct*, which includes rules regarding staff use of digital devices. The Designated Safeguarding Lead covers certain safeguarding-related aspects of IT in his induction training, such as: the importance of not using personal devices to create and store images of pupils; not accepting pupil friend requests on social media; only using pupil and staff e-mail accounts to send e-mails to students.

24. A summary of the *Acceptable Use of IT Policy* appears on the landing page when staff use the internet for the first time that day and has to be acknowledged before browsing can commence.

Visitors' use of computers, mobile 'phones and other digital devices

25. Visitors can request access to the School's Wi-Fi but must register for a temporary account that will enable their internet usage to be linked to them personally. By default, such accounts expire after 24 hours, although a longer expiry period can be agreed.

26. Our Code of Conduct for contractors stipulates that photographs of pupils must not be taken under any circumstances.

27. At the beginning of concerts and other similar events, parents who wish to photograph their children while performing are asked not to post images to social media.

28. There are signs in the swimming pool stating that photography of any kind is forbidden.

Training staff in online safety

29. Online safety is covered as part of staff safeguarding induction training.

30. The *Working Together to Safeguard Children* training delivered to all staff annually always covers online safety.

31. Members of the Safeguarding Team, especially the Online Safety Co-ordinator and DSL, communicate with staff about online safety, either in Staff Briefing or by e-mail, when something relevant happens in school or there is a national development of which staff should be aware.

Educating pupils in online safety

32. Online safety is covered in an age-appropriate fashion during Year 7 and Year 9 PSHE.

33. The Online Safety Co-ordinator speaks to the Upper School at least once a year about how to stay safe online.

34. Representatives from the RAP (Raising Awareness and Prevention) Project speak to every Upper School pupil about the dangers of social media and online pornography, particularly how the latter contributes to ingrained misogyny.

35. In September 2021, the DSL used the occasion of a spike in VPN use to write to the pupils involved to educate them about the dangers involved in this.

Advice to parents regarding online safety

36. From time to time representatives from the RAP (Raising Awareness and Prevention) Project are invited in to speak to all Upper School parents about the dangers of social media and online pornography, particularly how the latter contributes to ingrained misogyny.

37. The Online Safety Co-ordinator sends home ~~regular updates and suggested links regarding e-safety in the Senior School newsletter~~a monthly e-Safety Newsletter to parents in order to raise awareness. Recent topics include SafeToNet (an app that alert parents to concerning internet use by their children) and OnlyFans (a video posting and live streaming site that can lure children into creating increasingly sexualised content in order to earn money).

~~37.~~38. The DSL writes home to parents if there is a particular issue of concern. One such example was the rise in popularity among our pupils of anonymous and unmoderated chat-rooms such 'Monkey' that are designed to appeal to children but attract older men. Another was a surge in VPN use by pupils.

Appendix A – Social Media policy, rules and guidelines for pupil use of social media

Commented [SB2]: Developed in response to recent incidents

Day pupils

While on the School's premises social media use is forbidden for most pupils because a) mobile 'phones are not allowed to be used during the school day (unless with staff permission) b) social media sites are blocked using the School's wi-fi 0800-1700.

However, we need rules for use of devices:

- immediately before and after school using 4G etc.
- for Sixth-Formers when in free time in Sixth Form Centre using 4G etc.
- on school trips
- at fixtures
- on school transport

These are:

1. Never live-stream content without the explicit permission of a member of staff (mindful that live-streaming makes it impossible to 'undo' a mistake)
2. Do not create / post content that would make the School recognisable without first speaking to the Marketing Department or your Head of Section
3. Only create / post appropriate content- no swearing or indecent images, nothing that could be interpreted as sexually provocative, and in general nothing against the letter or spirit of the *Pupil Code of Conduct* or *Behaviour Policy*
4. Only use personal devices and your own 4G to create / post content: you must never use a Virtual Private Network (VPN) in conjunction with the School's wi-fi in order to access social media, nor should you try to use a School device (e.g. iPad) for this purpose

Boarders

The School is rightly concerned that social media sites allow for contact with strangers who could attempt to groom its pupils. That said, social media is an important part of young people's lives, and we do not wish to disadvantage boarders just because they happen to be boarders rather day pupils. More than that, some boarders may have a talent for curating an online presence and could make a living out of it in the future. More widely, we want to ensure that no boarder is denied access to sites that are safe; we also want to encourage pupils to work with our Marketing Department to capture exciting and authentic experiences of Freemen's school life.

Therefore:

- We block all irresponsible and obviously harmful social media sites for all boarders e.g. Omeagle, Monkey
- Responsible social media sites where there is recognised to be some 'stranger danger' are enabled for Sixth-Formers but not for boarders in Years 9-11

- We meet regularly with boarders to ask them which sites they want to use, and then assess risk. Our default is to unblock rather than block.
- This commitment comes hand in hand with an expectation on them not to use VPNs
- We educate all boarders on online safety so that they know how to use social media safely

The following rules apply to uploads to unblocked social media:

1. Never live-stream content without the explicit permission of a member of Walbrook staff (mindful that live-streaming makes it impossible to 'undo' a mistake)
2. Do not create / post content that would make the School recognisable without first speaking to the Marketing Department or the Head of Boarding
3. Only create / post appropriate content- no swearing or indecent images, nothing that could be interpreted as sexually provocative, and in general nothing against the letter or spirit of the *Pupil Code of Conduct* or *Behaviour Policy*
4. If you wish to create or post audio/visual content beyond the privacy of own bedroom, get permission from a member of Walbrook staff (informal / verbal permission is fine)
5. Never use a VPN to access social media

Pupil use of social media outside the School's jurisdiction

The parental contract states that the *Behaviour Policy* applies "at time and places in circumstances where failing to apply this policy may… have repercussions for the orderly running of the School or bring the School into disrepute." Pupils should be mindful of this when taking to social media.