Committee(s)	**Dated:**
The Board of Governors of the City of London Freemen's School For information/for decision	21st November, 2019.
Subject: Headmaster's Report on Policies	**Public**
Report of: Headmaster, City of London Freemen's School	**For Information**

Summary

This report is for Governor engagement and decision.

a) Background
b) Recommendation

Recommendation(s)

Members are asked to:

- Note the policies presented.

Main Report

a) Background

1. Members will understand that they are responsible for the School's policies and that oversight of them is an important part of their duties.

2. Two policies approved at the recent sub-committee meetings are considered of significance to the full Board of Governors:
   Appendix 1: Data Protection Policy
   Appendix 2: Onliine Safety Policy

b) Recommendation

FOR DECISION

3. It is recommended that Governors note the approved policies included as appendices in this report.

Appendices

- *Appendix 1*: Data Protection Policy
- *Appendix 2*: Online Safety Policy

Roland Martin
Headmaster

T: 01372 822 453/07747 563 634
E: Roland.Martin@cityoflondon.gov.uk
Tw: @RJMHM

Freemen's
Learn, lead and make a difference

CITY OF LONDON FREEMEN'S SCHOOL

Data Protection Policy

Data Protection Policy for both the Junior School and Senior School

Version number	2.01
Name and appointment of owner / author	Jo Moore (Bursar) / Anna Atkins (HR Manager)
Review Body	SLT, Finance, General Purposes & Estates Sub-committee and Full Board of Governors
Last updated	8th November, 2019
Reason for update	periodic review
Last reviewed by SLT	October 2019
Last reviewed by Governors	November 2019 (FGP&E Sub-committee)
Next SLT review due	July 2022
Next Governor review due	November 2019 (Full Board)
Where available	staff handbook, Parent Portal (restricted area of website)

Freemen's
Learn, lead and make a difference

CITY OF LONDON FREEMEN'S SCHOOL

CITY OF LONDON
FREEMEN'S SCHOOL

PUPIL & PARENT DATA PROTECTION POLICY

General Statement of the Duties of the City and the School

1. The City of London Corporation ('the City') is the data controller for the City of London Freemen's School ('the CLFS'), the City of London School ('the CLS'), the City of London School for Girls ('the CLSG') and the Guildhall Young Artists Division ('Junior Guildhall & Centre for Young Musicians') of the Guildhall School of Music & Drama. This Policy applies to personal information held and processed by the City of London Freemen's School.

2. The City, and the Schools, are required to process personal data regarding pupils, their parents and guardians as part of their operation, and will take all reasonable steps to do so in accordance with this Policy, the General Data Protection Regulations 2016 ('GDPR') and the Data Protection Act 2018 ('the DPA'). The City aims to have transparent systems for holding and processing written personal data. Any reference to personal data in this Policy includes reference to sensitive personal data. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

3. Any individual is entitled to request access to information relating to their personal data held by the schools. In this Policy any reference to pupils includes current, past or prospective pupils.

The Data Protection Act 2018

4. The City, and therefore each of the Schools, has the responsibility to comply with the DPA.

5. The DPA applies to information relating to both "personal" and "sensitive personal" data.

6. **Personal Data** is defined in the DPA as information relating to and identifying a living individual ("data subject"). The Schools may process a wide range of personal data of pupils, their parents or guardians, as part of their operation. To qualify as personal data, the data must be biographical in a significant sense, having the data subject as its focus and affecting the data subject's privacy. Personal data includes facts, any expression of opinion about an individual and any indication of the intentions of anyone in respect of that individual. Examples of personal data are: names and addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.

7. **Special categories of personal data** means personal data which reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, generic biometric and health data, information relating to a data subject's sex life or sexual orientation, criminal convictions and alleged offences.

8. In order to comply with the DPA the School must comply with the six Data Protection Principles which state that personal data:

   i. Will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
   ii. Will be collected only for specified, explicit and legitimate purposes; and it must not then be further processed in any manner incompatible with those purposes.
   iii. Will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
   iv. Will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
   v. Will not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.
   vi. Will be processed in a manner that ensures its appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9. **Processing** includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data.

Processing of Personal Data

10. Consent may be required for the processing of personal data unless the processing is necessary for the Schools to undertake their obligations to pupils and their parents or guardians. Personal data, unless otherwise exempt from restrictions on processing under the DPA, will only be disclosed to third parties under the terms of this Policy or otherwise with the consent of the appropriate individual.

11. The rights in relation to personal data set out under the DPA are those of the individual to whom the data relates. The Schools will, in most cases, rely on parental or guardian consent to process data relating to pupils unless, given the nature of the processing in question, and the pupil's age and understanding, it is unreasonable in all the circumstances to rely on the parent or guardian's consent. Parents should be aware that in such situations they may not be consulted.

12. Consent must be freely given, can be freely withdrawn and will generally be recorded by the individual's signed agreement.

Exemptions which Allow Disclosure of Personal Data to Third Parties

13. There are a number of exemptions in the DPA which allow disclosure of personal data to third parties, and the processing of personal data by the School and its employees, which would otherwise be prohibited under the DPA. The majority of these exemptions only allow disclosure and processing of personal data where specific conditions are met, namely:

    (a) the data subjects have given their consent (with regard to special categories of data, this may require explicit, written consent, depending on the circumstances);
    (b) for the prevention or detection of crime;
    (c) for the assessment of any tax or duty;
    (d) where it is necessary to exercise a right or obligation conferred or imposed by law upon the City or the Schools (other than an obligation imposed by contract);
    (e) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
    (f) for the purpose of obtaining legal advice;
    (g) for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress).

Use of Personal Information by the Schools

14. It is required under the DPA that the personal data held about pupils must only be used for specific purposes allowed by law. The School holds personal data on pupils. The personal data includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

15. The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing, together with any other uses normally associated with this provision in an independent school environment.

16. The School may make use of limited personal data (such as contact details) relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School.

17. In particular, the School may:

    (a) transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the School;
    (b) with parental consent, make use of photographs of pupils in School publications and on the School website;
    (c) with parental consent, disclose photographs and names of pupils to the media (or allow the media to take photographs of pupils) for promotional and congratulatory purposes where a pupil may be identified by name when the photograph is published e.g. where a pupil has won an award or has otherwise excelled;
    (d) make personal data, including sensitive personal data, available to staff for planning curricular or extra curricular activities;
    (e) keep the pupil's previous school informed of his/her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the school to his previous school.

18. Any wish to limit or object to any use of personal data should be notified to the Bursar of the relevant School in writing, which notice will be acknowledged by the School in writing. Parents who do not want their child's photograph or image to appear in any of the School's promotional material, or be otherwise published, must also make sure their child knows this.

19. Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use the DPA will not apply e.g. where a parent takes a photograph of their child and some friends taking part in the School sports day.

Disclosure of Personal Data to Third Parties

20. The School may receive requests from third parties (i.e. those other than the data subject, the School, and employees of the School) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the DPA which allows disclosure applies (see paragraph 12); or where necessary for the legitimate interests of the individual concerned or the School.

21. The following are the most usual reasons that the School may have for passing personal data to third parties:

    (a) to give a confidential reference relating to a pupil;
    (b) to give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend;
    (c) to publish the results of public examinations or other achievements of pupils of the School;
    (d) to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
    (e) to provide information to another educational establishment to which a pupil is transferring;
    (f) to provide information to the Examination Authority as part of the examinations process; and
    (g) to provide the relevant Government Department concerned with national education. At the time of the writing of this Policy, the government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

22. The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government departments or agencies strictly for statistical or research purposes.

23. Any wish to limit or object to any use of personal data by third parties, except as stated in paragraph 21 above, should be notified to the Bursar of the relevant School in writing, or to the relevant authority (the contact details for which can be supplied by the School).

24. Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

Accuracy of Personal Data

25. The City and the Schools will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the relevant School's Bursar in writing of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

Security of Personal Data

26. The City and the Schools will take reasonable steps to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this Policy and their duties under the DPA. The City and the Schools will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Retention of Personal Data

27. The Schools will have retention policies in place to ensure that personal data processed for any purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes.

Deletion of personal data

28. Where personal information is to be disposed of, the School will ensure that it is destroyed permanently and securely. This may involve the permanent removal of the information from the server so that it does not remain in a person's inbox, deleted items folder or recover deleted items folder, or, in the case of hard copies, shredding.

Rights of Access by Data Subjects to their Personal Data

29. Under the DPA, individuals have a right of access to their personal data held by the City and the Schools. This is known as a "subject access request" and is subject to exemptions and constraints within the DPA. Any request in writing will be responded to as long as satisfactory identification is given and the information request is clear.

Requests for Access to Records (Subject Access Requests)

30. A subject access request must be made in writing. Where the request is not complete or clear, or satisfactory identification has not been given, a request for clarification must be sent to the individual concerned within **two** working days of when the request is received by the School.

31. All requests for access to records must be placed on the relevant pupil's file, and the City's Information Compliance Team informed that the request has been received.

Responding to Requests for Access to Records

32. All requests for access to records must be passed to the Bursar.

33. The Headmaster or, in his absence, the Bursar must authorise the applicant's request for access before **any** information is disclosed (see also paragraphs 39-43 below).

34. The School will take advice from the Information Compliance Team or the Comptroller and City Solicitor in relation to disclosure.

35. All SARs must be acknowledged. The School must respond to a SAR, subject to any exemptions or constraints to disclosure, within one month from the date it is received. In some cases, such as where we process large amounts of the individual's data, we may respond within three months of the date on which the request is received. The Bursar will write to the individual within one month of receiving the original request to tell him/her if this is the case.

36. The DPA requires a response to a request to be given within **one calendar month** of the written request being received. The response period does not begin until:

    (a) a written application is received by anyone within the City of London Corporation (not when it has been passed on to and received by the Headmaster, Bursar, City's Information Compliance Team or the Comptroller and City Solicitor);
    (b) the School has received sufficient information to enable it to identify the individual who is seeking access;

(c) the School has received sufficient information to enable it to access the information requested; and

37. Where the conditions set out in paragraph 36 are fulfilled, in responding to the request, the School must confirm whether personal data is being processed and where that is the case, give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data is or may be disclosed. The School must also provide, in an intelligible form, a copy of the information held and, where possible, details of the source of the information. Finally, where processing results in automated decision making which evaluates matters relating to the data subject (for example, in the marking of multiple choice questions), the data subject should be informed and informed also of the logic involved in that decision-making.

38. Data subjects are not entitled to information where exemptions to the right of access apply (see paragraphs 56-60 below). Moreover, in these circumstances, the School must only give a notification to the data subject that no information has been identified which is required to be supplied under the DPA.

Authorisation of Access to Records on Behalf of a Child or Young Person

39. A child or young person may appoint a person with parental responsibility for him or her to request access to their records. In such circumstances the School must have written evidence that the child or young person has authorised the person with parental responsibility to make the application.

40. The Headmaster or, in his absence, the Bursar will determine what information will be shared with the person with parental responsibility. Access to records will be refused in instances where, for example, information sharing may place a child at risk of significant harm or jeopardise police investigations into any alleged offence(s).

41. Where a child or young person does **not** have sufficient understanding to make his or her own request, a person with parental responsibility can make a request on their behalf. The Headmaster or, in his absence, the Bursar must, however, be satisfied that:

(a) the child or young person lacks sufficient understanding; and
(b) the request made on behalf of the child or young person is in their interests.

42. The School will only grant pupils' access to their personal data if, in the relevant School's reasonable belief, the pupil understands the nature of the request. It is generally accepted that, by the age of 13, a child can be expected to have sufficient maturity to understand the nature of the request.

43. Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils.

Disclosure of Information

44. Any individual is, subject to exemptions and constraints within the DPA, entitled to have access to all information specifically held about him or her where:

(a) it is automated data being personal data held or processed electronically, for example, on a computer, word processor, audio and video system or telephone logging system;
(b) it is manual data which consists of non-automated information such as paper or microfiche files or records, which record information as part of a relevant filing system. A relevant filing system is defined as a set of information relating to individuals and structured either by reference to individuals or specific criteria relating to those individuals, so that specific information relating to a particular individual is readily accessible in a way broadly equivalent to information accessed within a computerised system.

45. The personal data must be provided in permanent form (e.g. paper, microfiche, CCTV images) unless:

(a) the supply of such a copy is not possible;
(b) supplying it in permanent form would involve disproportionate effort (in which case another way of viewing the data must be agreed with the applicant); or
(c) the data subject agrees otherwise.

46. Only relevant documents from the pupil's file will be duplicated and disclosed to the applicant who, if requested, should be given a copy of the duplicated document.

47. An individual is not entitled to information where:

(a) exemptions to the right of access apply (see paragraphs 56-60 below); or
(b) another person, including any family member, has not given their written consent to disclose information that identifies them (**but** see paragraph 49 below) .

48. Information contained in an individual's records is likely to contain information about persons other than the individual. Generally, information about or identifying another person must not be disclosed to the individual seeking access to the information without that person's written consent.

49. There may be circumstances where the Headmaster or, in his absence, the Bursar considers it *reasonable in all the circumstances* to disclose information without the consent of the other person. For example, when the person cannot be traced.

50. In determining what is reasonable in all the circumstances it is necessary to have regard to:

(a) any duty of confidentiality owed to the other person;
(b) any steps taken with a view to seeking consent of the other person to the disclosure;
(c) whether the other person is capable of giving consent; and
(d) any express refusal of consent by the other person.

51. In instances where the Headmaster or, in his absence, the Bursar have decided information concerning other people, or their identities may not be disclosed, it is acceptable to blank out the relevant information.

52. There is also a general presumption in favour of disclosing personal data relating to individuals, where this information is integral to the personal data of the applicant. So, the records kept by teachers in the course of their employment in respect of pupils may be disclosable.

53. Any request by an individual for access to information held about them must be complied with subject to this paragraph and to the exemptions set out in paragraphs 56-60 below. The School may, however, make a request for more specific details of the information sought.

54. A request for access to files without the permission of the individual must be directed to the Information Compliance Team or the Comptroller and City Solicitor.

55. A record of the information disclosed in response to a request for access to information should be kept on the pupil's file, including details of any exemptions to disclosure relied upon (see paragraphs 56-60 below).

Exemptions to Access by Data Subjects

56. Confidential references given, or to be given by the Schools, are exempt from access. The Schools will therefore treat as exempt any reference given by them for the purpose of the education, training or employment, or prospective education, training or employment of any pupil.

57. It should be noted that confidential references received from other parties may also be exempt from disclosure, under the common law of confidence. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

58. Examination scripts, that is information recorded by pupils during an examination, are exempt from disclosure. However, any comments recorded by the examiner in the margins of the script are not exempt even though they may not seem of much value without the script itself.

59. Examination marks do not fall within an exemption as such. However, the one calendar month compliance period for responding to a request is extended in relation to examination marks to either five months from the day on which the School received the request (if all the necessary conditions set out in paragraph 36 are fulfilled), or one calendar from the announcement of the examination results, whichever is the earlier.

60. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is exempt from disclosure unless the privilege is waived.

Repeated Requests for Access to Records

61. Unless a reasonable period of time has lapsed between the compliance with one request and receipt of the next, under the DPA the School is not obliged to comply with subsequent identical or similar requests from that applicant.

Complaints

62. If an individual believes that the relevant School has not complied with this Policy or acted in accordance with the DPA they should utilise the relevant School's complaints procedure.

63. If the individual is still not satisfied, they may make representations to the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel (01626) 545 700.

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	1.01
Name and appointment of owner / author	Stuart Bachelor, Deputy Head and Designated Safeguarding Lead
Review Body	Safeguarding Team, SLT, Finance, General Purposes & Estates Sub-committee and Full Board of Governors
Last updated	8th November, 2019
Reason for update	n/a- new policy
Last reviewed by SLT	October 2019
Last reviewed by Governors	November 2019 (FGP&E Sub-committee)
Next Safeguarding Team review due	September 2020
Next SLT review due	July 2021
Next Governor review due	November 2019 (Full Board)
Where available	Staff Handbook, Parent Handbook (restricted area of website)

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* (2019), identifies three main types of online risk faced by children:

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

   • C**ontact**: 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.

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* (2019), Stuart Bachelor, in his role as Designated Safeguarding Lead, takes lead responsibility for online safety.

   The Safeguarding Team, which comprises the DSL and eight Deputy Designated Safeguarding Leads, meets half-termly to discuss both the operational and strategic aspects of safeguarding, including online safety. Richard Dolan, DDSL and Head of Sixth Form, is a trained CEOP Ambassador with a particular interest in and wider knowledge of online safety. The Head of Boarding, Jemima Edney, is also a DDSL and therefore well positioned to take the lead on online safety in Walbrook.

   Adam Cohen 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
   - 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 youth-produced sexual imagery (YPSI) and not deleting it immediately;
- creating YPSI;
- disseminating YPSI without consent;
- soliciting YPSI.

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.

Youth-produced sexual imagery (YPSI)

8. The School takes YPSI 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 can be found in Section 24 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. Richard Dolan 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.

Pupil personal data and images

13. 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

14. *Keeping Children Safe in Education* states: "Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises."

15. 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 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

16. 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.

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

Virtual Private Networks (VPNs)

18. 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*).

19. 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. 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.

20. Experience suggests that VPNs tend to be used by boarders for undesirable rather than nefarious or harmful purposes. In an effort to minimise VPN use and its attendant safeguarding risks, boarding staff promote a culture of honesty and compromise regarding sites that boarders would like to be unblocked.

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

21. 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.

22. 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

23. 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.

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

25. 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.

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

Training staff in online safety

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

28. The *Working Together to Safeguard Children* training delivered to all staff in August 2019 included discussion of several scenarios related to online safety, including YPSI, use of VPNs and exposure to extremist online content.

29. Richard Dolan, drawing on his CEOP training, has used Staff Briefings to update all staff on recent developments in online safety- e.g. what the latest apps are and how they are being used by students. Similarly, Janet Wilby-King (DDSL) in 2018-19 used a slot to talk to staff about safe pupil use of social media and how we can support pupils in this respect.

Educating pupils in online safety

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

31. Following a series of YPSI incidents, the DSL spoke to all pupils in Year 9 and above concerning the legal, disciplinary and personal consequences of YPSI.

32. Richard Dolan speaks to the Sixth Form at least once a year about how to stay safe online.

33. On 1/2/19 representatives from the RAP (Raising Awareness and Prevention) Project were invited in to speak to all Year 10 and 11 pupils about the dangers of social media and online pornography, particularly how the latter contributes to ingrained misogyny.

Advice to parents regarding online safety

34. On 31/1/19 representatives from the RAP (Raising Awareness and Prevention) Project were 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.

35. Richard Dolan sends home regular updates and suggested links regarding e-safety in the Senior School newsletter.