On-Line Safety Policy

Bancroft's

Independent Co-educational Day School 7–18

Contents

1 Aims 1
2 Scope and application 1
3 Regulatory framework 1
4 Publication and availability 3
5 Definitions 3
6 Responsibility statement and allocation of tasks 3
7 Filtering and Monitoring 4
8 Role of staff and parents 4
9 Access to the School's technology 7
10 Procedures for dealing with incidents of misuse 10
11 Education 11
12 Training 13
13 Cybercrime 15
14 Risk assessment 16
15 Record keeping 17
Appendix one 18
Additional information relevant to the Prep School 18

1 Aims

1.1 This is the online safety policy of Bancroft's (**School**) including the Preparatory and Senior School.

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which empowers the School to:

1.2.1 protect the whole school community from potentially illegal, inappropriate and harmful content or contact;

1.2.2 educate the whole school community about their access to and use of technology;

1.2.3 establish effective mechanisms to identify, intervene in and escalate concerns where appropriate; and

1.2.4 help to promote a whole school culture of openness, safety, equality and protection.

1.3 This policy forms part of the School's whole school approach to promoting child safeguarding and wellbeing, which involves everyone at the School and seeks to ensure that the best interests of pupils underpins and is at the forefront of all decisions, systems, processes and policies.

1.4 Online safety is recognised as a safeguarding issue and forms part of the School's whole-school safeguarding culture. The School acknowledges that technology is a significant component in many safeguarding and well being concerns and that children may be exposed to risk both online and offline.

1.5 Online safety is a running and interrelated theme throughout the devising and implementation of many of the School's policies and procedures (including its safeguarding (child protection) policy and procedures) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead.

1.6 Although this policy is necessarily detailed, it is important that our safeguarding related policies and procedures are transparent, clear and easy to understand for staff, pupils, parents and carers. The School welcomes feedback on how we can continue to improve our policies.

2 Scope and application

2.1 This policy applies to the whole School with specific reference to the Prep School in Appendix 1.

2.2 This policy applies to all members of the school community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off school premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the school community or where the culture or reputation of the School is put at risk.

3 Regulatory framework

3.1 This policy has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 Education and Skills Act 2008;

3.1.3 Children Act 1989;

3.1.4 Childcare Act 2006;

3.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (**UK GDPR**); and

3.1.6 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (**KCSIE**);

3.2.2 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media and Sport (DfDCMS) and UK Council for Internet Safety (UKCIS), December 2020 updated March 2024);

3.2.3 Revised Prevent duty guidance: for England and Wales (Home Office, April 2023, updated March 24);

3.2.4 Channel duty guidance: Protecting people susceptible to radicalisation (Home Office, October 2023, updated October 2025;

3.2.5 Behaviour in schools: advice for headteachers and school staff 2022 (DfE, September 2022);

3.2.6 Searching, screening and confiscation: advice for Headteachers, school staff and governing bodies (DfE, July 2022 in force from September 2022);

3.2.7 Safeguarding children and protecting professionals in early years settings: online safety considerations (UKCIS, February 2019);

3.2.8 Relationships Education, Relationships and Sex Education (**RSE**) and Health Education guidance (DfE, July 2025 and effective from September 2026);

3.3 The following School policies, procedures and resource materials are relevant to this policy:

3.3.1 Pupil Acceptable Use of IT and Digital Technologies policy

3.3.2 Staff IT acceptable use policy;

3.3.3 Safeguarding (child protection) policy and procedures;

3.3.4 Anti-bullying policy;

3.3.5 Behaviour, Rewards and Sanctions Policy;

3.3.6 Staff code of conduct and whistleblowing policy;

3.3.7 Data protection policy for staff;

3.3.8 School rules and procedures;

3.3.9 Relationships and sex education policy.

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from The Head's PA or the School Office during the School day.

4.4 This policy can be made available in large print or other accessible format if required.

5 Definitions

5.1 Where the following words or phrases are used in this policy:

5.2 References to the **Board of Governors** are references to the proprietor of the School.

5.3 Reference to **staff** includes all those who work for or on behalf of the School, regardless of their employment status, including contractors, supply staff, volunteers and Governors unless otherwise indicated.

5.4 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

6 Responsibility statement and allocation of tasks

6.1 The Board of Governors has overall responsibility for all matters which are the subject of this policy

6.2 The Board of Governors is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Board of Governors' response to this duty.

6.3 Governors will seek assurance that filtering and monitoring systems are operating effectively and that safeguarding arrangements reflect current statutory guidance, emerging technologies and online.

6.4 To ensure the efficient discharge of its responsibilities under this policy, the Board of Governors has allocated the following tasks:

Task	**Allocated to**	**When / frequency of review**
Keeping the policy up to date and compliant with the law and best practice	IT Director & Designated Safeguarding Lead	As required, and at least termly
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of	IT Director & Designated Safeguarding Lead	As required, and at least termly

internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness		
Online safety	Designated Safeguarding Lead	As required, and at least annually
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	Designated Safeguarding Lead IT Steering Group	As required, and at least annually
Formal annual review	Board of Governors	Annually

7 Filtering and Monitoring

7.1 The School recognises that effective filtering and monitoring are an essential part of safeguarding. Appropriate filtering and monitoring systems are in place to safeguard pupils from harmful and inappropriate content and to identify safeguarding concerns that may arise through the use of technology.

7.2 The Designated Safeguarding Lead, IT leadership and Senior Leadership Team will work together to ensure that filtering and monitoring systems are effective, proportionate and responsive to safeguarding risks.

7.3 The School will ensure that:

7.3.1 filtering and monitoring arrangements are reviewed at least annually;

7.3.2 governors receive appropriate assurance regarding filtering and monitoring arrangements;

7.3.3 safeguarding implications are considered whenever new technologies are introduced;

7.3.4 systems are capable of identifying safeguarding concerns;

7.3.5 staff know how to report concerns regarding filtering and monitoring systems;

7.3.6 identified concerns are acted upon promptly and appropriately.

8 Role of staff and parents

8.1 Head and Senior Leadership Team

8.1.1 The Head has overall executive responsibility for the safety and welfare of members of the School community.

8.1.2 The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead

includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's safeguarding (child protection) policy and procedures.

8.1.3 The Designated Safeguarding Lead will work with the IT Director (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

8.1.4 Filtering and monitoring arrangements will be reviewed at least annually and whenever significant technological or safeguarding developments occur. Monitoring arrangements will include consideration of emerging technologies, AI-enabled services, anonymising tools and any mechanisms that may enable users to bypass existing safeguards

8.1.5 The Designated Safeguarding Lead will ensure that concerns relating to generative AI, deepfakes, digitally manipulated imagery, AI-facilitated bullying, impersonation, exploitation, harassment or misinformation are managed through the School's safeguarding procedures in the same way as other online safety concerns.

8.1.6 The Designated Safeguarding Lead will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

8.2 **IT Director**

8.2.1 The IT Director, together with his / her team, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

8.2.2 The IT Director is responsible for ensuring that:

(a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the School's technology if they are properly authenticated and authorised;

(c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;

(d) Filtering and monitoring arrangements will be reviewed at least annually and whenever significant technological or safeguarding developments occur. Monitoring arrangements will include consideration of emerging technologies, AI-enabled services, anonymising tools and any mechanisms that may enable users to bypass existing safeguards

(e) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

(f) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(g) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

8.2.3 The IT Director will report regularly to the Senior Leadership Team on the operation of the School's technology. If the IT Director has concerns about the functionality, effectiveness, appropriateness or use of technology within the School, including of the monitoring and filtering systems in place, he / she will escalate those concerns promptly to the Designated Safeguarding Lead.

8.2.4 The IT Director is responsible for maintaining the safeguarding log] (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's safeguarding (child protection) policy and procedures.

8.3 **All staff**

8.3.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

8.3.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

8.3.3 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

8.3.4 Staff should understand how generative AI technologies may contribute to safeguarding concerns, including the creation or circulation of deepfake images, AI-generated sexualised imagery, impersonation, misinformation, bullying, harassment or exploitation. Staff should be alert to indicators that AI may have been involved in an incident and report concerns promptly in accordance with safeguarding procedures.

8.3.5 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic or misandrist messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content;

(d) cyberbullying.

8.3.6 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and / or encourages physical abuse;

(b) facilitates, threatens and / or encourages sexual violence; or

(c) is used as part of initiation / hazing type violence and rituals.

8.3.7 It is important that staff recognise the indicators and signs of child- on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

8.3.8 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst-case scenario, a culture that normalises abuse.

8.3.9 The School has a **zero-tolerance approach** towards child-on-child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's behaviour, rewards and sanctions policy and as a safeguarding matter under the School's safeguarding (child protection) policy and procedures.

8.3.10 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's safeguarding (child protection) policy and procedure. If staff have any concerns regarding child-on-child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the Designated Safeguarding Lead in all cases**.

8.4 **Parents**

8.4.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents to promote safe practice when using technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

8.4.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead.

9 Access to the School's technology

9.1 The School provides internet, intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using school technology. All such use is monitored by the IT team.

9.2 Pupils and staff require individual user names and passwords to access the School's internet, intranet and email system which must not be disclosed to any other person. Any pupil or

member of staff who has a problem with their user names or passwords must report it to the IT team immediately.

9.3 No laptop or other mobile electronic device may be connected to the School network without the consent of the IT Director. The use of any device connected to the School's network will be logged and monitored by the IT team. See also 9.5 below and the School's information security policy (including remote working and bring your own device to work).

9.4 The School has a separate wireless network connection available for use by visitors to the School. A visitor is required to register via the "BSch-Visitor" SSID Portal; this emails an approval request to the IT helpdesk who will authorise the user if appropriate. Use of this service will be logged and monitored by the IT team.

9.5 **Inappropriate material**

9.5.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

9.5.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead. The term 'online safety' encapsulates a wide range of ever evolving issues but these can be classified into four main areas of risk:

(i) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,);

(ii) **Contact** - being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,

(iii) **Conduct** - online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and online bullying; and

(iv) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group risks such as online gambling, inappropriate advertising, phishing and or financial scams.

9.5.3 The School recognises that AI technologies may create risks across all four categories of online safety (Content, Contact, Conduct and Commerce), including exposure to AI-generated harmful content, interactions with AI chatbots, creation of manipulated images and videos, misinformation, disinformation, fraud and impersonation.

9.6 **Use of mobile electronic devices and smart technology**

9.6.1 The School does all that it reasonably can to limit children's exposure to the risks identified above through the use of the School's IT system.

9.6.2 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email text messaging and social media sites) when connected to the School's network, and their effectiveness is regularly reviewed.

9.6.3 Mobile devices and smart technology equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. The School is alert to the risks that such access presents, including the risk of pupils sexually harassing, bullying or controlling their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually (often via large group chats); or viewing and / or sharing pornography and other harmful content, and has mechanisms in place to manage such risks.

9.7 Pupils should be aware that AI-enabled applications accessed through personal devices may collect personal information, generate inaccurate information, produce harmful content or be used to create manipulated images or recordings of others. Use of such technologies in ways that harm members of the School community may result in disciplinary and safeguarding action.

9.7.1 Details of current filtering and monitoring safeguarding controls are maintained by the School and reviewed regularly by safeguarding and I.T leads

9.7.2 In certain circumstances, a pupil may be given permission to use their own mobile device or other smart technology to connect to the internet using the school's network. Permission to do so must be sought and given in advance.

9.7.3 The School rules about the use of mobile electronic devices or other smart technology, including access to open / non-School networks, are set out in the acceptable use policy for pupils.

9.7.4 The use of mobile electronic devices by staff is covered in the staff code of conduct, IT acceptable use policy, social media guidelines, data protection policy for staff and information security policy (including remote working and bring your own device to work). Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

9.7.5 The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

10 Procedures for dealing with incidents of misuse

10.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

10.2 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to shared further (e.g. with the Designated Safeguarding Lead) to discuss next steps.

10.3 **Misuse by pupils**

10.3.1 Anyone who has any concern about the misuse of technology by pupils should report it immediately so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-bullying	House staff including Tutors record incidents on CPOMS using appropriate categories. These will alert the Senior Tutor. Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Sharing nudes and semi-nude images (sexting / youth produced sexual imagery)	safeguarding (child protection) policy	All staff will refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Sexual violence and sexual harassment (whether during or outside of school)	safeguarding (child protection) policy	The Designated Safeguarding Lead who has overall responsibility for online safety matters
Harassment	safeguarding (child protection) policy	All staff will record on CPOMS which will alert the appropriate House Staff. Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Upskirting	safeguarding (child protection) policy	All staff will refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters

Radicalisation	safeguarding (child protection) policy	All staff will refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Other breach of acceptable use policy	See relevant policy referred to in acceptable use policy	Housemaster / Housemistress, Form Tutor / designated member of staff Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters

10.3.2 **Anyone** who has **any** concern about the welfare and safety of a pupil must report it **immediately** in accordance with the School's child protection procedures (see the School's safeguarding (child protection) policy).

10.4 **Misuse by staff**

10.4.1 If anyone has a safeguarding-related concern relating to staff misuse of technology, they must report it immediately in accordance with the School's policy on raising concerns and allegations which is set out in the safeguarding and child protection policy and procedures.

10.4.2 Anyone who has any other concern about the misuse of technology by staff should report their concerns as set out below:

(a) staff should speak to their Head of Department / Line Manager in accordance with the staff whistleblowing policy; and

(b) anyone else should speak to the Head.

10.5 **Misuse by any user**

10.5.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the IT Director or the Designated Safeguarding Lead.

10.5.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

10.5.3 If the School considers that any person is vulnerable to radicalisation, the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

11 Education

11.1 The teaching of online safety is integrated, aligned and considered as part of the whole-school safeguarding approach and wider staff training and curriculum planning.

11.2 The School ensures that children are taught how to keep themselves and others safe, including online, and the safe use of technology is therefore integral to the School's curriculum. Pupils are educated in an age appropriate manner about the importance of safe

and responsible use of technology, including the internet, social media and mobile electronic devices (see the School's curriculum policy).

11.3 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorials, workshops and pastoral activities, teaching pupils:

11.3.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

11.3.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";

11.3.3 to recognise AI-generated content, deepfakes, manipulated media, misinformation and disinformation;

11.3.4 to understand the benefits, limitations and safeguarding risks associated with generative AI technologies;

11.3.5 to use AI technologies safely, critically, ethically and responsibly;

11.3.6 to understand the importance of protecting personal data when using AI services and online platforms

11.3.7 how to recognise suspicious, bullying or extremist behaviour;

11.3.8 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

11.3.9 the consequences of negative online behaviour;

11.3.10 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

11.3.11 how to respond to harmful online challenges and hoaxes.

11.4 The School recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole-school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, misogyny/misandry, homophobia, biphobia and sexual violence and sexual harassment.

11.5 Pupils are taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The School has a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's behaviour, rewards and sanctions policy] and also as a safeguarding matter under the School's safeguarding (child protection) policy and procedures.

11.6 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

11.7 The School's acceptable use of IT and Digital technologies policy for pupils sets out the School rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

11.8 The School recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils. For more details on the School's approach, see School's child protection and safeguarding policy and procedures and relationships education /RSE/ PSHE and Learning for Life programme.

11.9 Useful online safety resources for pupils;

11.9.1 http://www.thinkuknow.co.uk/

11.9.2 http://www.childnet.com/young-people

11.9.3 https://www.saferinternet.org.uk/advice-centre/young-people

11.9.4 http://www.safetynetkids.org.uk/

11.9.5 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

11.9.6 https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people

12 Training

12.1 Board of Governors

12.1.1 To ensure that all Governors are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of the School are effective and that they support the delivery of a robust whole school approach to safeguarding, all Governors receive appropriate safeguarding and child protection (including online safety) training at induction. This training is regularly updated.

12.2 Staff

12.2.1 The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

12.2.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy.

12.2.3 Staff training is regularly updated and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. Staff training will also include awareness of emerging technologies and generative artificial intelligence, including AI-generated imagery, deepfakes, misinformation, impersonation, data protection considerations and safeguarding risks associated with AI-enabled applications. This training may be in addition to the regular safeguarding and child protection (including online safety) updates as required at induction and at least annually thereafter.

12.2.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology., and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

12.2.5 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in the School's safeguarding (child protection policy and Procedures and Searching, screening and confiscation: advice for schools (DfE, January 2018). In certain cases, it may be appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

12.2.6 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' where safeguarding is concerned, including in relation to sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and / or violent behaviour in the future.

12.2.7 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and / or staff training will be delivered to minimise the risk of it happening again.

12.2.8 Staff also receive data protection training on induction and at regular intervals afterwards.

12.2.9 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

12.2.10 **Useful online safety resources for staff**

(a) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

(b) http://www.childnet.com/teachers-and-professionals

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(d) https://www.thinkuknow.co.uk/teachers/

(e) http://educateagainsthate.com/

(f) Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, December 2020 updated March 2024).

(g) SELMA Hack online hate toolkit

12.2.11 The Redbridge local safeguarding partnership has produced guidance for parents on radicalisation which is available here: Guidance on Radicalisation and Extremism – Redbridge Safeguarding Children Partnership (redbridgescp.org.uk).

12.3 **Parents**

12.3.1 The School is in regular contact with parents and carers and uses its communications to reinforce the importance of ensuring that children are safe online. The School aims to help parents understand what systems are in place to filter and monitor their child's online use and ensures that parents are aware of what their children are being asked to do online (including what sites they will be asked to access) and who from the School they will be interacting with online, if anyone.

12.3.2 Periodically the Pastoral Office arrange webinars for parents on a range of topics including the use of and risks associated with IT.

12.3.3 Parents are encouraged to read the acceptable use policy for pupils with their son / daughter to ensure that it is fully understood.

12.3.4 **Useful online safety resources for parents**

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

(b) http://www.childnet.com/parents-and-carers

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(d) https://www.thinkuknow.co.uk/parents/

(e) https://www.ceop.police.uk/safety-centre

13 Cybercrime

13.1 Cybercrime is criminal activity committed using computers and / or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

13.2 Cyber-dependent crimes include:

13.2.1 unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

13.2.2 denial of service (Dos or DDoS) attacks or 'booting', which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

13.2.3 making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

13.3 The School recognises that cyber security forms an important part of safeguarding. Staff and pupils will be educated regarding phishing, social engineering, identity theft, account compromise, ransomware and other cyber threats that may place children, staff or School systems at risk

13.4 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

13.5 If staff have any concerns about a child in this area, they should refer the matter to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

13.6 Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding / Anti Bullying / Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

14 Risk assessment

14.1 The School recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The School will carry out regular, and at least annual, reviews of its approach to online safety, supported by risk assessments which consider and reflect the risks face by their pupils. These reviews will include consideration of emerging digital risks, including artificial intelligence technologies, deepfakes, online misinformation, cyber security threats and changing patterns of online behaviour among children and young people.

14.2 Furthermore, where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

14.3 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

14.4 The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

14.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Designated Safeguarding Lead who has been properly trained in, and tasked with, carrying out the particular assessment.

15 Record keeping

15.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

15.2 All concerns raised through the School's filtering and monitoring reporting will be logged initially on CPOMS

15.3 All serious incidents involving the use of technology will be logged centrally and advised to the Designated Safeguarding Lead who will maintain the Safeguarding Incident Log.

15.4 The records created in accordance with this policy may contain personal data. The School's use of this personal data will be in accordance with data protection law. The School has published on its website privacy notices which explain how the School will use personal data.

Appendix one

Additional information relevant to the Prep School

The Whole School policy on On-line Safety sets out clearly the attitude and approach taken by Bancroft's to protecting children and young people when they use digital technologies; it also sets out important guidance for staff. The children in the Prep School are younger, but the policy applies to us too, although some practices and points of emphasis may be different to those of the Senior School.

At Bancroft's Prep School we are determined to keep the children safe in the digital world. To this end the School seeks to ensure that appropriate controls are in place to prevent accidental or deliberate access of inappropriate sites and material. Where Prep children attempt to do so, this is flagged up by the system so that the Prep Head is informed and can take appropriate action.

Older Prep pupils who travel independently to school are allowed to bring in mobile phones if their parents make a written request for them to do so. These are handed in to the Prep office on arrival and collected on departure. This means that Prep children can only access the internet when at school via our PCs and tablets not their own devices.

As part of their Computing and PSHEE lessons, the children are taught how to be responsible users of technology- for example by keeping their user names and passwords safe and secure. We also have regular assemblies and workshops delivered by providers such as the NSPCC and the UK Safer Internet Centre to educate the children about staying safe on line. Inset for staff and talks to parents delivered by SWGfl ensure that the adults in the children's lives are aware of issues which can arise when children use various apps and social media outside school, especially those which are not age appropriate.

Through informing staff and parents, and empowering children to use digital technologies confidently and responsibly we aim to keep them safe. Children are aware of 'stranger danger' when communicating on-line and know not to disclose or share personal information. They also know to report any unpleasant or inappropriate material or messages, or indeed anything that makes them feel uncomfortable when they are on-line.

Digital technologies have become integral to our lives. These technologies are powerful tools which open up new opportunities for everyone. They can stimulate discussion, promote creativity and significantly enhance learning. At Bancroft's Prep School we believe that children have an entitlement to safe internet access at all times.