CRANFORD
SCHOOL

Whole School E-Safety Policy

Please also refer to the **'Whole School Anti-Bullying Policy and Procedures', 'Whole School Safeguarding and Child Protection Policy', 'Whole School Safeguarding and Child Protection Procedures', 'IT Code of Conduct for Pupils', 'Personal Mobile Devices Policy for Senior School Pupils', 'Preventing Radicalisation Policy (Including EYFS)'** and **'Policy for the Use of Smartphones and Cameras in the EYFS (Includes Photography Policy)'.**

Policy Statement:

Cranford School is aware of the growing evidence of the mismatch between the high levels of exposure pupils have to digital devices and their low awareness of safety issues involved. For this reason, E-Safety is embedded into the curriculum based on the '4Cs' (Content/ Contact/ Conduct/ Commerce) and all staff ensure that use of digital devices is closely monitored. Training is organised for staff as well as parents to help them understand the importance of online safety.

This policy is available in the Cranford School Policies section of the Whole School Staff Teams area on Microsoft Teams for all staff to read. It is also available to all interested parties on the School website. The policy is reviewed annually, and when events or legislation requires, by the Headmaster and Director of Senior School Data. The School review the Child protection and Safeguarding Policy and Procedures, including online safety, annually, and to make sure the procedures and implementation are reviewed regularly. The next review date is September 2024.

The Headmaster ensures that online safety training is included in staff safeguarding and child protection training. He also ensures the safe use of technology, mobile phones and cameras in the whole school, including the early years setting.

Guiding Principles:

Our E-Safety Policy is based on the '4Cs' as outlined below. The School recognises its duty to safeguard pupils from current and potential risks both in and out of school.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

1. **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. **Contact**: being subjected to harmful online interaction with other users; 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.

3. **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
4. **Commerce -** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel pupils, or staff are at risk, this should be reported to the DSL. They may report it to the Anti-Phishing Working Group (https://apwg.org/).

IT in the Curriculum:

Technology has transformed the entire process of teaching and learning at Cranford School. It is a crucial component of every academic subject and is also taught as a subject in its own right. The majority of the School's classrooms are equipped with electronic whiteboards, projectors and at least one teacher workstation. Cranford School has two IT Suites in the School and Senior School pupils may use their own devices for private study and when working in lessons. The school uses a Smoothwall web filter to control and manage web access by pupils and staff.

Pupils are taught how to research on the Internet and to evaluate sources. They are educated to understand the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution. Some websites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic, extremist or other propaganda. Some free, online encyclopaedias do not evaluate or screen the material posted on them.

This includes staying safe online and the dangers of cyberbullying and sharing nudes and semi-nudes (as outlined in the 'Whole School Internet Safety Policy.') We recognise that many pupils are able to have unlimited and unrestricted access to the internet using their own data plan both in school and out of school: which some of them may abuse to sexually harass their peers, share indecent images and non-consensually and view and share pornography and other harmful content. To minimise inappropriate use, as a school we ensure all pupils, with their parents, sign an acceptable use code of conduct, '**IT Code of Conduct for Pupils (Junior and Senior)**'.

The Role of Technology in our Pupils' Lives:

Technology plays an enormously important part in the lives of all young people. Smartphones, tablets, Chromebook/laptops, desktop PCs and games consoles (such as PlayStation, Xbox and Wii) provide unlimited access to the internet. SMS messages, social media websites (like X and Facebook), VoIP (video calls, via web cameras built into devices using software such as Skype), wikis (collaborative web pages), chat rooms, social networking applications (such as Tik Tok, Instagram, Snapchat, Be Real, Bebo, and Facebook), and video sharing sites (such as YouTube) are all technological media to which pupils are exposed.

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the School's role to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, cyber-bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

Role of IT Staff:

The School recognises that blocking and barring sites is no longer adequate. Staff teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a particular responsibility of the School's Safeguarding Leads and its pastoral staff. The School's Network Director and IT staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for training the School's teaching and support staff in the use of IT. They monitor the use of the Internet and emails and will report inappropriate usage to the pastoral staff. Computing teaching staff use resources promoted by DfE to cover the use of social media for on-line radicalisation: www.saferinternet.org.uk (the UK Safer Internet Centre) and www.thinkuknow.co.uk (CEOP's website).

Role of the Safeguarding Leads:

Cranford School recognises that Internet safety is a child protection and general safeguarding issue.

Our Safeguarding Leads have been trained in the safety issues involved with the misuse of the Internet and other digital technologies. They work closely with the Local Safeguarding Children Board (OSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of Cranford School. The School has a comprehensive Personal, Social, Health, Citizenship and Economic Education (PSHCEE) eSafety programme and it is embedded in the Computing curriculum.

The DSL takes the lead and is responsible for ensuring that all staff receive adequate training is part of their safeguarding and online safety training to ensure that they understand their expectations, roles and responsibilities around filtering and monitoring systems.

All pupils in the School are educated (age-appropriately) in the risks and the reasons why they need to behave responsibly online. Allegations of misuse of the Internet must be brought to the immediate attention of the Headmaster.

All members of the Cranford School community, including governors recognise that Internet safety is a child protection and general safeguarding issue.

Role of Governors:

- Make sure that the school has appropriate filtering and monitoring systems in place and review their effectiveness
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers about what needs to be done to support the school to meet these standards
- Make sure the DSL takes lead responsibility for understanding the filtering and monitoring systems in place as part of their role
- Make sure that all staff undergo safeguarding and child protection training, including online safety, and that such training is regularly updated and in line with advice from the safeguarding partners
- Make sure staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training

Sen Misuse:

Cranford School will not tolerate any illegal material and will always report illegal activity to the police and/or the OSCB. Junior School (Years 3 - 6) and Senior School Pupils are required to sign a **'Network Code of Practice and Email Code of Practice'/'IT Code of Conduct for Pupils'** detailing their responsibilities for the safe use of IT in School.

Parents are required to countersign the agreements. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our '**Whole School Anti-Bullying Policy and Procedures'**.

Involvement with Parents and Guardians:

Cranford School seeks to work closely with parents and guardians/carers in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School. The School recognises that not all parents and guardians/carers may feel equipped to protect their son or daughter when they use digital technologies at home. The School therefore arranges an information and discussion evening for parents when an outside specialist advises about the potential hazards of this technology and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

The school uses communications with parents and carers to reinforce the importance of children being safe online. The information shared with parents/ carers includes information about:

- what systems they have in place to filter and monitor online use
- what they are asking children to do online, including the sites they will ask to access
- who from the school (if anyone) their child is going to be interacting with online.

The School also recognises the importance of educating parents and carers about children's access to online sites when away from school.

Procedures:

E-safety is a Whole School responsibility and at Cranford School we follow the procedures below to maintain a culture of safety in the use of IT equipment:

Safety Measures:

- The School filters and monitors online activity via applications which prevent access to blocked internet sites, and report on attempts to access sites that may give rise to concern.
- Email messages between staff and students are also scanned for inappropriate language and behaviour. This information is shared with the DSL who follows up on any concerns.
- The School ensures staff have a school owned office 365 account for conducting all school business.

- The School deals with issues of confidentiality, information sharing and consent as indicated in the **"Whole School Privacy Policy."**

Cyber-bullying:

- Cyber-bullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place.
- The School's **'Whole School Anti-bullying Policy and Procedures'** describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe IT environment at School but everyone needs to learn how to stay safe outside the School. The strong pastoral support system, coupled with the PSHCEE and Computing Schemes of Learning, assist in educating pupils about the risks involved and in keeping them safe.
- Cranford School values all of its pupils equally. It is part of the ethos of the School to promote considerate behaviour and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating Other Users with Respect:

- The School expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact.
- The School expects a degree of formality in communications between staff and pupils and would not normally expect them to communicate with each other by text or smartphones. The School's '**Whole School Outings and Trips Policy'** and **'Whole School Outings and Trips Procedures'** explains the circumstances when communication by smartphone may be appropriate. In such circumstances, staff use School, as opposed to personal, phones. Pupils' mobile numbers are deleted at the end of the visit and pupils are instructed to delete staff numbers.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The **'Whole School AntiBullying Policy and Procedures'** is available to parents on the School website. The School is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of staff.
- Smartphones are not permitted in School unless the pupil travels to and from School by School minibus, in which case phones are collected and kept in the main School Office during the day and returned on the return home. As a privilege, Year 11, Year 12 and Year 13 pupils are permitted to use their phones in their respective Common Rooms only. They may, however, use their devices in lessons with the express permission of their teacher from whom this permission must first be sought.

Keeping the School Network Safe:

- The School adheres to best practice regarding teaching Computing and use of the Internet.

- Staff must adhere to the '**Network Code of Practice for Staff**', '**Social Media Policy**' and the **'Electronic Communication and Internet Policy Statement'**.
- Certain sites are blocked by the School's filtering system and the School's Network Director and IT staff monitor pupils' use of the network. Cranford School is conscious of the need to ensure that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The IT Team regularly test the operation of the web filtering solution and will inform the Headmaster and DSL of the time and date of these tests and record them for future referral. The IT team monitors email traffic and our email provider and our endpoint provider block spam and certain attachments.
- The DSL and governors are aware of their responsibility with regards to filtering and **m**onitoring systems and take this seriously ensuring the pupils safety at all times.
- The School issues all pupils in Years 3 to 11 with their own personal School email address. Access is via personal login, which is password protected. The School gives guidance on the reasons for always logging off and for keeping all passwords secure.
- The School has strong anti-malware protection on its network which is operated by the Network Director.

Promoting Safe Use of Technology:

Pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Childnet International (https://www.childnet.com/)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyber-bullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

PSHCEE and Computing Schemes of Learning cover the different hazards of the Internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving oneself from future embarrassment, explaining that any comment or photograph posted online is there permanently. Anything that has been deleted may be cached in a search engine, company server or Internet archive and cause embarrassment years later.

Safe Use of Personal Digital Devices:

We recognise that many pupils are able to have unlimited and unrestricted access to the internet using their own data plan both in school and out of school: which some of them may abuse or misuse. To minimise inappropriate use, as a school we ensure all pupils, with their parents, sign an acceptable use code of conduct, **'IT Code of Conduct for Pupils (Junior and Senior)'. The** school restricts unsupervised use of mobile phones during all times in the school day. Mobile phones are not permitted in School unless the pupil travels to and from School by School minibus, in which case phones are collected and kept in the main School Office during the day and returned on the return home. As a privilege, Year 11, Year 12 and Year 13 pupils are permitted to use their phones in their respective Common Rooms only. They may, however, use their devices in lessons with the express permission of their teacher from whom this permission must first be sought.

- The School's guidance is that pupils and staff should always think carefully before they post any information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- The School offers guidance on the safe use of social networking sites and cyber-bullying in PSHCEE and Computing lessons which covers blocking and removing contacts from 'friend lists'.
- The School's PSHCEE and Computing lessons include guidance on how pupils can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online.
- The School offers guidance on keeping names, addresses, passwords, phone numbers and other personal details safe. Privacy is essential in the online world.
- The School organises a talk to parents from CEOP who give guidance on how to keep safe at home by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content.
- Similarly, the School covers how a smartphone filter can be activated and how to block nuisance callers.

Considerate Use of Electronic Equipment:

- Staff may confiscate personal equipment that is being used during the School day.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

Reviewed: September 2019: Headmaster and Director of IT
Reviewed: September 2020: Headmaster and Director of IT
Reviewed: September 2021: Headmaster and Director of IT (and Assistant Head, Academic)
Reviewed: September 2022 by Headmaster, Deputy Head (DSL) and Director of IT
Reviewed: September 2023 by Headmaster, Deputy Head (Whole School and DSL) and Director of Senior School Data
Reviewed: March 2024 by Headmaster, Deputy Head (Whole School and DSL) and Director of Senior School Data
Review Due: September 2024 by Headmaster, DSL, Director of Senior School Data