**CHRIST'S HOSPITAL**

ONLINE SAFETY POLICY

Introduction

1. Online safety has been defined by Ofsted as: "a school's ability to protect and educate students and staff in their use of technology as well as having appropriate mechanisms in place to intervene and support any incident where appropriate."

2. Promoting a safe online culture and protecting students involves using appropriate monitoring and filtering to control what students can access when using the School's network to access the internet.

3. However, education about online safety is the only way to ensure that, wherever they are, students know how to stay safe online.

Scope

4. Students, staff (teaching and support) and parents represent three core communities where Christ's Hospital should be proactive in ensuring that we all derive and follow best practice in relation to online safety. Through recognising and utilising our collective knowledge, professionalism and experience, we can continue to make good progress.
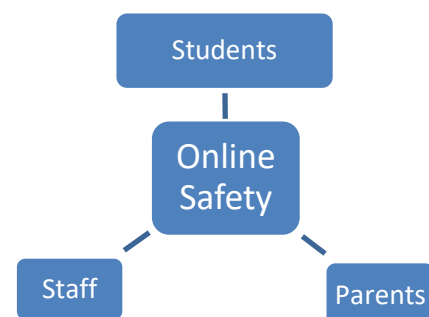
5. We aim to reduce the risks presented by:

    - online bullying;
    - grooming and exploitation;
    - youth-produced sexual imagery ("sexting");
    - inappropriate use of social media;
    - damage to online reputation;
    - access to inappropriate web content;
        - material of a sexual nature
        - extreme violence
        - material intended to exert extreme influence over (radicalise) the viewer
        - misuse of identity, personal information, and identity theft
    - overuse, lack of self-control and poor habits;
    - carelessness with personal online security such that misuse by others is facilitated;
    - hacking;
    - lack of awareness of potential consequences.

    We also recognise that it is important that, owing to the very fluid nature of the internet and online use, we keep abreast of the latest trends in use. This applies especially to the use of social media.

Practice

6. Students in the Second and Third Forms are not allowed to use social media, including WhatsApp, to communicate with other Christ's Hospital students, other than their own siblings, whilst at School. This is because experience has shown that, despite the online safety education provided, our youngest students all too easily slip into habits of thoughtless or unkind messaging, causing serious upset to others.

7. Education pertaining to online safety takes place:

<u>For students</u>

- When it is appropriate in the classroom. For example, when a class is researching, appropriate attention should be drawn to validity and bias.
- In specific programmes within Learning for Life and PSHE. This begins in the Second Form.
- In the ICT Code of Conduct for Students.
- On an ad hoc basis in tutorials, for example bringing the attention of tutor groups to stories in the press which pertain to online safety and are age relevant.
- By inviting guest speakers and specialists to talk to specific year groups; for example, addressing the Deputy Grecians (Year 12) on the importance of 'online reputation', within the Senior Learning for Life programme and the Second and Third Form students on the detrimental effects of misuse or overuse of social media in the Junior Learning for Life programme.
- By interacting with other subjects. For example, working with the drama department to create and perform short pieces on online bullying.
- By creating responsibilities for students; junior students are given opportunities to create online safety materials in Learning for Life and PSHE lessons.
- By listening to students' concerns and harnessing 'student voice' via School and House Councils and other student forums.
- By utilising the School website and portal to host and display relevant information such as 'Safer Internet Day'.

<u>For staff</u>

- Through specialised INSET and CPD. For example, raising staff awareness of good practice with social media. Staff need to know about risks and safeguarding in this area for themselves and also for the students.
- Staff are also regularly reminded about good practice as part of annual safeguarding INSET.
- Staff are directed to report concerns which they may have about usage.

<u>For parents</u>

- Utilising areas of the CH website and/or Parents' Portal to host information relevant to parents on online safety. Provision of resources: links to specialist websites, news articles and our policies at CH.
- Inviting parents to presentations by guest speakers at events such as Parents' Pastoral Mornings; dissemination of online safety advice.
- Parental communications covering updates to the School's policies and new concerns about evolving online safety issues.

Sanctions

7. <u>Students</u>

- School sanctions such as Saturday evening Head of Year detention, suspension, Deputy Head's Behavioural Agreement or Head Teacher's contract can and will be used in support of online safety.
- Students are informed that the above sanctions will be used in cases of online bullying, posting inappropriate images or comments online or misuse of social media. <u>These activities will not be tolerated.</u>
- The ultimate sanction is expulsion, either for a repeat of behaviour that has already incurred a more minor sanction or for a single instance of very serious misuse of the internet, including social media.

Technical online safety arrangements

8. The following technical online safety measures are in place at Christ's Hospital:

    - ICT Codes of Conduct are in force for both staff and students.
    - User access controls (log-ins and complex passwords).
    - MFA (*Multi-Factor Authentication*) applied to all network accounts when accessing School IT resources from outside the School
    - Regularly updated anti-virus and other security software.
    - Network level security user restrictions.
    - Encryption of email and portable devices.
    - Monitoring and filtering of email.
    - Internet web page access controls, including monitoring and filtering of all sites accessed by staff and students.
    - Managed wireless user controls.
    - Physical server and data centre access controls.

10. It is accepted that exceptionally, for good educational reasons, students may need to research certain topics (e.g. racism, drugs, discrimination etc.) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT team temporarily remove those sites from the filtered list for the period of study. Any request to do so is referred to the Deputy Head. Any such decision will be auditable, with clear reasons for the need.

Investigating incidents and breaches

11. Any actual or suspected online safety incidents that put the safety of a student at risk should be reported without delay to the School's Designated Safeguarding Lead and the Deputy Head who will initiate the appropriate reporting and investigative actions.

12. Breaches of this policy by students and other incidents, which do not present an immediate threat to the safety of students or staff, should be reported to the Head of Year who will then take the appropriate action. Serious search breaches by students will be reported to the Deputy Head.

13 The Deputy Head will review an online safety report every day, during term time. Action, either directly with the student or through the house parent and/or Designated Safeguarding Lead, will be taken where necessary.

Monitoring and review

13. The effective implementation of this policy will be assessed regularly by the Deputy Head.

Associated policies

14. This policy should be read in conjunction with the following documents, copies of which are available on the School intranet (for staff) and/or website:

    - Child Protection and Safeguarding Policy
    - Information Security and Data Protection Policy
    - ICT Code of Conduct for Students
    - ICT Code of Conduct for Staff

Author: RMJB/DJS
Date of last review: June 2023
Date of next review: June 2024