RYDES HILL PREPARATORY SCHOOL & NURSERY

P50 (ISI 7H) – ONLINE SAFETY POLICY

RYDES HILL
PREPARATORY SCHOOL & NURSERY

MISSION STATEMENT

- Rydes Hill Preparatory School and Nursery is a Catholic school where children learn how to live in loving relationship with God and each other.
- Christian virtues of love and justice, faith and courage, hope and perseverance are fostered.
- Pupils and staff comprise individuals of different faiths and beliefs but the Rydes Hill community aspires to unity within the life of the school based on shared moral values.
- The importance placed on the development of individual talents is at the heart of what school stands for and all are encouraged and challenged to be the best they can be.

Written By :	Sarah Norville - Headmistress	4th September 2018
Reviewed By :	Alison Packman – Compliance Officer	27th September 2018
Approved By :	Vanessa Wood – Deputy Head (Pastoral)	4th October 2018
Governor Review By :	Not required	

Contents

Revision History

Revision	Paragraph Number	Revision
November 2015		Original document
November 2016		Update
June 2018	Whole document	Reformatted to include revision history, paragraph numbers, Abbreviation, Acronym and Definitions table. Updated staff names where relevant staff have left the school. References to "P03 Use of ICT, Mobile Phones and Other Electrical Equipment Policy" amended to "P03 Computing, Mobile Phones & Electronic Devices Policy". References to "e-safety" have been replaced with "online safety"
	Front page	Updated Logo & Mission Statement.
	Paragraph 3	Update to policy titles and numbers. Addition of P41 and P54 to list.
	Paragraph 6	Add "i-pads"
	Paragraph 9	Updated reference to KCSIE document issue date
	Paragraph 25	Sentence relating to i-pads added
	Paragraph 27	Replaced
	Paragraph 38	Delete "Data Protection Act 1998" and replace with "General Data Protection Regulations 2018"
	Paragraph 48	Final line added

Abbreviations, Acronyms and Definitions

Abbreviation / Acronym	Definition
EYFS	Early Years Foundation Stage
GDPR	General Data Protection Regulations 2018
Parents	Birth parents, adoptive parents, step-parents or any other adult with parental responsibility for the child
School community	Current, prospective and former Parents, current, prospective and former Pupils, current, prospective and former Staff, current and former Governors.
SLT	Senior Leadership Team
Staff	Full-time and part-time personnel working at the School whether employed by them directly or not (i.e. includes peripatetic staff, visiting coaches and tutors, volunteers etc.)

Aim / Objective / Statement of Intent

This policy applies to the whole school including EYFS.

1. It is the duty of Rydes Hill Preparatory School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including, but not limited to, the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

2. New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

    - Websites;
    - Email and instant messaging;
    - Blogs;
    - Social networking sites;
    - Chat rooms;
    - Music / video downloads;
    - Gaming sites;
    - Text messaging and picture messaging;
    - Video calls;
    - Podcasting;
    - Online communities via games consoles; and
    - Mobile internet devices such as smart phones and tablets.

3. This policy, supported by the P03 – Computing, Mobile Phones & Electronic Devices Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

    - P01 - Anti-Bullying Policy;
    - P04 - Safeguarding Policy;
    - P09 - Taking, Storing and Using Images of Pupils & Staff Policy;
    - P16 - Behaviour, Rewards, Sanctions and Use of Reasonable Force Policy;
    - P38 - Health and Safety Policy;
    - P41 – Data Retention Policy;
    - P44 - PSHCE Curriculum Policy;
    - P48 - Social Media Policy; and
    - P53 - Privacy Notice for Parents & Pupils;
    - P54 – Privacy Notice for Job Applicants, Staff, Governors & Volunteers

4. Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

5. At Rydes Hill Preparatory School we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

6. Both this policy and the P03 – Computing, Mobile Phones & Electronic Devices Policy cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, i-pads etc.); as well as all devices owned by pupils and staff brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and Responsibilities

7. The Online Safety Coordinator, Mrs Vanessa Wood, the Designated Safeguarding Lead (DSL) Mrs Sarah Norville, the Senior Leadership Team and the IT coordinator (Mrs Di Morris) have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current online safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

8. Rydes Hill Preparatory School believes that it is essential for parents / carers to be fully involved with promoting online safety both in and outside of school. We consult and discuss online safety with parents / carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

9. This policy also takes account of the updated version of Keeping Children Safe in Education September 2018.

10. It is essential that children are safeguarded from potentially harmful and inappropriate online material. As such governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place.

11. The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation- technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

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

    - content: being exposed to illegal, inappropriate or harmful material
    - contact: being subjected to harmful online interaction with other users
    - conduct: personal online behaviour that increases the likelihood of, or causes, harm
        i. proprietors should ensure that as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Staff awareness

13. New staff receive information on Rydes Hill's Online Safety and P03 – Computing, Mobile Phones & Electronic Devices Policy as part of their induction. All teaching staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors also receive our Online Safety Policy on arrival at school.

14. All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. These behaviours are summarised in the P03 – Computing, Mobile Phones & Electronic Devices Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

15. Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

16. A record of concern must be completed by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's Online Safety Coordinator (Mrs Vanessa Wood) and the DSL (Mrs Sarah Norville).

Online safety in the curriculum and school community

17. IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful

basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

18. The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHCE, as well as informally when opportunities arise.

19. At age-appropriate levels, usually via ICT and PSHCE lessons, pupils are taught to look after their own online safety. From Kindergarten class pupils are formally and informally taught about recognising online exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL - Mrs Norville, the online Safety Coordinator – Mrs Vanessa Wood and any member of staff at the school.

20. From Kindergarten pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.

21. 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 Anti-bullying Policy). Pupils should approach Mrs Norville, Mrs Wood, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Use of School and personal devices

Staff

22. School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

23. Staff at Rydes Hill are permitted to bring in personal devices for their own use. Staff must ensure their mobile phones are on ‘silent’ during the working day. They may use their mobile telephone only during break-times and lunchtimes. Staff are reminded of the school’s policy (P09 Taking, Storing and Using Images of Children and Staff) relating to images.

24. Personal telephone numbers may not be shared with pupils or parents / carers and staff may not contact a pupil or parent / carer using a personal telephone number. The only exception to the above is contact with parents/carers (not pupils) on off-site trips or sporting events.

Pupils

25. Mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored in the IT suite or in classrooms. I-pads are stored in specialist charging units in the corridors. Access is available via the pupils' Form Tutor or the ICT Coordinators (Mrs Di Morris).

26. No personal devices belonging to pupils should be at school. If pupils bring in mobile phones because they are going to another parent's home over the weekend, they should be handed into their form teacher in the morning where they can be locked away until home time.

Use of internet and email

Staff

27. Limited use of email and Internet facilities for personal purposes is permitted so long as this is not during lesson time. The School acknowledges that personal use may occur from time to time. Any such use must be in accordance with this Policy and must not disrupt staff duties. Abuse or excessive use of the e-mail and/or internet will be dealt with through the disciplinary procedure.

28. When accessed from personal devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

29. There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored.

30. Staff must immediately report to the Online Safety Coordinator (Mrs Vanessa Wood) the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

31. Any online communications must not either knowingly or recklessly:

    - place a child or young person at risk of harm;
    - bring Rydes Hill School into disrepute;
    - breach confidentiality;
    - breach copyright;
    - breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- use social media to bully another individual; or
- post links or material which is discriminatory or offensive.

32. Under no circumstances should school pupils or parents be added as social network 'friends'.

33. Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

34. There is strong anti-virus and firewall protection on our network. Pupils are not required to use emails in school. There is no reason why a pupil should send an email to school unless it is work that they are sending to their teacher's work email address. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work purposes, pupils should contact their form teacher for assistance.

35. Pupils should immediately report, to Mrs Vanessa Wood, the Online Safety Coordinator / IT Manager, Mrs Di Morris or another member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

36. Pupils must report any accidental access to materials of a violent or sexual nature directly to a member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's P16 - Behaviour, Rewards, Sanctions and Use of Reasonable Force Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

37. Certain websites are automatically blocked by the school's filtering system.

Data Storage

38. The school takes its compliance with the General Data Protection Regulations 2018 (GDPR) seriously. Please refer to the School's Privacy Notices (P53 & P54) and P03 – Computing, Mobile Phones & Electronic Devices Policy for further details.

39. Staff are expected to save all data relating to their work to their school laptop/ PC or to the school's central server as per the IT Policy.

40. Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier, to be encrypted before sending.

41. Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the School.

42. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Headmistress.

Password Security

43. Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

44. All pupils and members of staff should:

    - use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every [3] months;
    - not write passwords down; and
    - should not share passwords with other pupils or staff.

Safe use of digital and video images

45. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

46. When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

47. In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by GDPR). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), nor should parents / carers comment on any activities involving other pupils in the digital / video images.

48. Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy, P03 – Computing, Mobile Phones & Electronic Devices Policy and P09 – Taking, Storing and Using Images of Pupils and Staff Policy, concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes except for under the specific conditions allowed for in P09.

49. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

50. Pupils must not take, use, share, publish or distribute images of others without their permission.

51. Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school.

52. Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Complaints

53. As with all issues of safety at Rydes Hill School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Headmistress and the e-Safety Coordinator, Mrs Vanessa Wood in the first instance, who will undertake an immediate investigation and liaise with the management team and any members of staff or pupils involved. Please see the Complaints Policy (P39) for further information.

54. Incidents of or concerns around online safety will be recorded using a Concern form and reported to the school's Online Safety Co-ordinator (Mrs Vanessa Wood) and the Designated Safeguarding Lead , Mrs Sarah Norville, in accordance with the school's Safeguarding Policy.