PARK SCHOOL – E-SAFETY POLICY

Park School believes that the use of information and communication technologies in schools brings great benefits. Recognising e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

1 WHO WILL WRITE AND REVIEW THE POLICY?

1.1 The school has appointed an e–Safety Coordinator who in conjunction with the Headteacher and Bursar will be responsible for writing/reviewing this policy.

1.2 This policy and its implementation will be reviewed annually.

1.3 This policy has been agreed by the school's senior management team.

2 DEFINITION OF ONLINE SAFETY CONCERNS (KCSIE 2021)

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

2.1.1 content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

2.1.2 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'.

2.1.3 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

2.1.4 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 (https://apwg.org/).

3 TEACHING AND LEARNING

3.1 Why is Internet use important?

3.1.1 Internet use is part of the Park School curriculum, enhances learning and is an invaluable tool used by pupils and staff for a wide range of educational and administration purposes.

3.1.2 The Internet is a part of everyday life for education, business and social interaction.

3.1.3 Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

3.1.4 Internet access is an entitlement for students who show a responsible and mature approach to its use.

3.2 How will Internet use be controlled?

3.2.1 The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

3.2.2 Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

3.2.3 Staff should guide pupils to age-appropriate online activities that will support the learning

outcomes planned for the pupils' age and ability.

3.2.4 Pupil access to the internet in school is always supervised and teacher-led where appropriate.

3.3 How will pupils learn how to find and evaluate Internet content?

3.3.1 Pupils will use age-appropriate tools to research Internet content (through the use of filters).

3.3.2 Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3.3.3 Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3.3.4 The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

4 MANAGING INFORMATION SYSTEMS

4.1 The e-safety coordinator carries out an annual review of the school's approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. This is completed using the 360 safe website tool.

4.2 How will our network be protected?

4.2.1 The security of the school information systems and users will be reviewed regularly.

4.2.2 Virus protection will be updated regularly.

4.2.3 Personal data sent over the Internet or taken off site will be encrypted.

4.2.4 Portable media may be not used without specific permission followed by an anti-virus / malware scan.

4.2.5 Unapproved software will not be allowed in work areas or attached to email.

4.2.6 The Bursar and IT Consultant will review system capacity regularly.

4.2.7 The use of user logins and passwords to access the school network will be enforced.

4.3 How will email be managed?

4.3.1 All email messages can be monitored and can be reviewed in the school's Email Archiving and eDiscovery system. Pupils are given training on the appropriate use of email.

4.3.2 Staff will only use official school provided email for work related purposes.

4.3.3 Staff will be given regular training relating to phishing email attacks and staff are encouraged to report suspicious emails to the IT department.

4.4 How will published content be managed?

4.4.1 The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

4.4.2 Email addresses will not be published online to avoid being harvested for spam.

4.4.3 The Headteacher & School Board have overall editorial responsibility for online content published by the school and ensures that content published is accurate and appropriate.

4.5 Can pupils' images or work be published?

4.5.1 Images or videos that include pupils will only be used with the agreement of their parents and in accordance with statutory regulations.

4.6 How will social networking, social media and personal publishing be managed?

4.6.1 The school will carefully control any access to social media and social networking sites.

4.6.2 Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Bursar before using Social Media tools in the classroom.

4.6.3 Any personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

4.6.4 Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

4.6.5 All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

4.6.6 Newsgroups are blocked for non-Admin staff and pupils unless a specific use is approved.

4.6.7 Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) may, if appropriate, be raised with their parents/carers.

4.7 How will filtering be managed?

4.7.1 The school's broadband internet access will include filtering appropriate to the age and maturity of pupils.

4.7.2 Filtering is carried out by a device which automatically updates multiple times each day as and when new threats are detected.

4.7.3 If staff or pupils discover any unsuitable sites or suspect that anyone is attempting to access content that should not be accessed, staff should report any confirmed of suspected breach of filtering on a "e-Safety Incident Form" (available from the ICT Suite or on Sharepoint). This form should be given to the e-Safety Co-ordinator who will record and escalate the concern as appropriate.

4.7.4 The School filtering system will block all sites on the Internet Watch Foundation (IWF) blacklist.

4.7.5 Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Bursar.

4.7.6 Regular checks are made by the IT support to ensure that the filtering methods selected are effective and confirmation of this is given regularly to the e-safety co-ordinator who shares this at each meeting of the ICT Committee.

4.7.7 Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Dorset Police or CEOP

4.7.8 The school's access strategy is decided upon on an ongoing basis to suit the age and curriculum requirements of the pupils.

4.8 How will video calls be managed?

4.8.1 Video calls may be used by staff in admin offices and in classrooms via Teams.

4.8.2 Video calls can be used in areas where children are for the purpose of sharing messages from the Office or to share activities across classrooms.

4.8.3 Video calls can only be made to Park School accounts unless prior permission has been agreed by the Headteacher or Bursar. Calls to external domains is specifically prevented except for those domains "white-listed". The IT Consultant will only white-list domains with

prior approval from the Bursar.

4.8.4 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.9 How should personal data be protected?

4.9.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and General Data Protection Regulations.

5 POLICY DECISIONS

5.1 How will Internet access be authorised?

5.1.1 The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

5.1.2 All staff will read and sign to confirm their understanding and agreement to the 'Staff ICT Acceptable Use Policy' before using any school ICT resources.

5.1.3 Parents are asked to read the 'Park School Computer and Internet Use – Notes and Guidelines for Parents' and discuss it with their child. This document is sent out on admission.

5.1.4 All visitors to the school site who require unsupervised access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy.

5.1.5 Visitors will never be allowed to log-in as a member of staff. A visitors wi-fi pass may be generated or they may be logged in to a school device using a specific generic log-in such as "interviewee". Such user logins are subject to enhanced security and do not have access to data within the general school network.

5.2 How will risks be assessed?

5.2.1 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Park School cannot accept liability for the material accessed, or any consequences resulting from Internet use.

5.2.2 The school regularly audits ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

5.2.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Dorset Police.

5.2.4 Methods to identify, assess and minimise risks will be reviewed regularly.

5.3 How will the school respond to any incidents of concern?

5.3.1 All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc) which will be done via the "e-Safety Incident Form".

5.3.2 The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log.

5.3.3 The Designated Safeguarding Leader will be informed of any relevant e-Safety incidents.

5.3.4 The school will manage e-Safety incidents in accordance with the school discipline/

behaviour policy where appropriate.

5.3.5 The school will inform parents/carers of any incidents of concerns as and when required.

5.3.6 After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

5.3.7 The relevant class teacher and, if appropriate, the Headteacher will be informed of any e-Safety incidents involving pastoral issues.

5.3.8 Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school may refer the concern to the Police.

5.3.9 The e-safety incident log will be reviewed by the ICT Committee at least annually in their meetings.

5.4 How will e–Safety complaints be handled?

5.4.1 Complaints about Internet misuse will be dealt with under the School's complaints procedure.

5.4.2 Any complaint about staff misuse will be referred to the Headteacher and Bursar.

5.4.3 A record of all e–Safety complaints will be maintained by the e-Safety Co-ordinator, including any actions taken.

5.4.4 Discussions may be held with the local Police Safer Schools Partnership Coordinators and/or the Local Authority's Children's Safeguarding Team to establish procedures for handling potentially illegal issues.

5.5 How will Cyberbullying be managed?

5.5.1 Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Bullying Policy.

5.6 Pupils' Use of Personal Devices

5.6.1 Mobile phones, cameras or other personal electronic devices are not permitted in school unless prior permission is given by the Headteacher for a specific purpose. Pupils' devices will not be accessible during the school day and will be kept in the school office.

5.6.2 If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office until returned to parents/carers.

5.7 Staff use of Personal Devices

5.7.1 See the Staff ICT Acceptable Use Policy.

6 COMMUNICATION OF E-SAFETY ISSUES

6.1 How will this policy be discussed with pupils?

6.1.1 All pupils will be informed that network and Internet use can be monitored and traced to the individual user.

6.1.2 An e–Safety training programme for pupils regularly raises the awareness and importance of safe and responsible internet use amongst pupils.

6.1.3 Pupil instruction regarding responsible and safe use of the Internet and the network is provided by staff wherever appropriate.

6.1.4 The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

6.1.5 All members of the school community, including parents/guardians will be reminded about

safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

6.1.6 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

6.2 How will the policy be discussed with staff?

6.2.1 The e–Safety Policy will be provided to and discussed with all members of staff upon joining the school.

6.2.2 Upon joining the School, staff sign and agree to comply with the Staff ICT Acceptable Use Policy.

6.2.3 Staff are made aware that Internet and network use can be monitored and traced to the individual user. Discretion and professional conduct is essential.

6.2.4 Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, is regularly provided.

6.2.5 Staff who manage filtering systems or monitor ICT use are supervised by the senior management and have clear procedures for reporting issues.

6.3 How will parents' support be enlisted?

6.3.1 Parents' attention is drawn to this policy when joining the school.

6.3.2 A partnership approach to e-Safety at home and at school with parents is encouraged. The school puts on regular events for parents and suggestions for safe home Internet use.

6.3.3 As part of the School's admissions procedures parents are asked to sign the document entitled 'Park School Computer and Internet Use – Notes and Guidelines for Parents.' By signing this document, parents confirm that they have discussed this issue with their child, and bind their child to using the Internet and the School's ICT systems within the limits set by the school.

6.3.4 Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet is regularly made available to parents.

6.3.5 Parents can be referred, where appropriate, to organisations listed in the "e–Safety Contacts and References section". (Appendix 1 of this policy.)

7 THE PREVENT DUTY

7.1 The school's safeguarding policy and procedures ensure that the school fulfils its statutory duties to have due regard to the need to prevent people from being drawn into being radicalised (including support for extremist ideas that are part of radicalised ideology). The school ensures that our pupils are safe from radicalisation and extremist material when accessing the internet in school, including by ensuring suitable filtering is in place. Internet safety is taught to the pupils in PSHE and ICT lessons and every teacher made aware of the possible risks posed by on-line activity of extremist and radicalisation groups. More details are contained in our safeguarding policy.

APPENDIX 1 - E-SAFETY CONTACTS AND REFERENCES

Additional references from KCSIE 2021 Annex D

CEOP (Child Exploitation and Online Protection Centre)	www.ceop.police.uk
Childline	www.childline.org.uk
Childnet	www.childnet.com
Children's Safeguarding Team	enquiries@bournemouth-poole-lscb.org.uk Tel: 01202 458 873 LSCB Admin Office, Bournemouth Learning Centre, Ensbury Avenue, Bournemouth, BH10 4HG
Click Clever Click Safe Campaign	http://clickcleverclicksafe.direct.gov.uk
Digizen	www.digizen.org.uk
Google Family Safety Centre	http://www.google.co.uk/goodtoknow/familysafety/
How to set up the parental controls offered by your Internet service provider (BT, Sky, TalkTalk and Virgin Media)	http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls
How to set up parental controls on any internet connection	https://goo.gl/dbWE1h
Internet Watch Foundation (IWF)	www.iwf.org.uk
Kidsmart	www.kidsmart.org.uk
Teach Today	http://en.teachtoday.eu
Think U Know website	www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse	www.virtualglobaltaskforce.com
UK Safer Internet Centre	http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers

Advice for governing bodies/proprietors and senior leaders

- **Childnet** provide guidance for schools on cyberbullying
- **Educateagainsthate** provides practical advice and support on protecting children from extremism and radicalisation
- **London Grid for Learning** provides advice on all aspects of a school or college's online safety arrangements
- **NSPCC** provides advice on all aspects of a school or college's online safety arrangements
- **Safer recruitment consortium "guidance for safe working practice"**, which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- **South West Grid** for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

- **UK Council for Internet Safety** have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- **Department for Digital, Culture, Media & Sport (DCMS)** - Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- **Department for Digital, Culture, Media & Sport (DCMS)** - A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- **London Grid for Learning** guidance, including platform specific advice
- **National Cyber Security Centre** guidance on choosing, configuring and deploying video conferencing
- **National Cyber Security Centre** guidance on how to set up and use video conferencing
- **UK Safer Internet Centre** guidance on safe remote learning

Support for children

- **Childline** for free and confidential advice
- **UK Safer Internet Centre** to report and remove harmful online content
- **CEOP** for advice on making a report about online abuse

Parental support

- **Childnet** offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- **Commonsensemedia** provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- **Internet Matters** provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- **Let's Talk About It** provides advice for parents and carers to keep children safe from online radicalisation
- **London Grid for Learning** provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- **Stopitnow** resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- **National Crime Agency/CEOP Thinkuknow** provides support for parents and carers to keep their children safe online 154
- **Net-aware** provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- **Parentzone** provides help for parents and carers on how to keep their children safe online
- Parent info from **Parentzone** and the **National Crime Agency** provides support and guidance for parents from leading experts and organisations
- **UK Safer Internet Centre** provide tips, advice, guides and other resources to help keep children safe online