RAYNES
PARK HIGH SCHOOL

E-Safety Policy

Statutory	No
Responsibility	Assistant Headteacher
Approval Authority	Governing Body – E-Safety Committee
Approval Date	December 2025
Next Review and Frequency	Autumn 2026
Monitoring and Evaluation	E-Safety Committee
Author	Assistant Headteacher, Mr P Nash
Availability	Every, Website
Version	Final
Equality Impact Statement	Yes

RAYNES PARK HIGH SCHOOL

Contents Page

Key People:	Designated Safeguarding Lead (DSL) team	Mr P Nash
	eSafety Coordinator	Mr D Jackson
	Link governor for safeguarding	Mrs T Benzecry
	eSafety Link Governor	Mrs H Capgras
	Network manager / other technical support	M N Martin
	Cybersecurity Link Governor	Mr S Liakat

RAYNES PARK HIGH SCHOOL

E-Safety Policy

Introduction

Today's students are growing up in a world where online and offline life is almost seamless. This offers many opportunities but also creates challenges, risks and threats. At Raynes Park High School we try to equip our students with the knowledge to be able to use technology to their best advantage in a safe, considered and respectful way.

Our school community recognises the importance of treating e-Safety as an ever-present serious safeguarding issue and its teaching as a whole school issue and the responsibility of all staff. It is important to protect and educate both students and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community.

Ofsted reviews e-Safety measures in schools and there are numerous Acts of Parliament which relate when considering the safeguarding of both staff and students in schools. The safeguarding aspects of e-Safety are evident in all our ICT/Safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review.

It is also critical to ensure the safety and security of all personal data that the school holds and processes. Under the General Data Protection Regulation, the school is responsible for exacting standards of safety and security of personal data that may be processed.

There is a clear guidance that clarifies how schools should address age verification requirements under the new Online Safety Act.

This policy links all the ICT, safeguarding and other policies and procedures to reflect how the school deals with e-Safety issues on a daily basis. The documents referred to in this e-Safety policy have been developed by various groups including:

Governors, including the link governor for safeguarding

Headteacher/Senior Leadership Team (SLT)/Designated Safeguarding Lead

E-Safety co-ordinator and ICT technical support staff

Teachers and support staff

Parents/carers

Student

It is essential that that Governing Bodies and proprietors should regularly review the effectiveness of school filters and monitoring systems. They should ensure that the leadership team and relevant staff are:

- aware of and understand the systems in place
- manage them effectively
- know how to escalate concerns when identified.

Schools and colleges should use communications with parents and carers to reinforce the importance of children being safe online. Schools should share information with parents/carers 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 or college (if anyone) their child is going to be interacting with online.

Objectives and targets

This policy is aimed at making the use of electronic communication at Raynes Park High School as safe as possible. This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

Online Safety is now categorised into four areas of risk (source section: 135 KCSIE):

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. Misinformation is the unintentional spread of this false or misleading content (Cabinet Office, Department for Science, Innovation and Technology, 2023).

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.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

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/).

Action plan

The school will deal with any e-Safety incidents which arise by invoking this policy, other ICT policies and the associated safeguarding, behaviour and anti-bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate e-Safety behaviour that take place out of school and take appropriate action.

The following sections outline:

- The roles and responsibilities for e-Safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles

- How the infrastructure is managed
- How e-Safety is considered in the curriculum
- The protocols on using digital images
- The protocols on data protection
- The protocols for handling electronic communication
- Awareness of and dealing with inappropriate use of electronic media

Roles and Responsibilities – Governors

- Filtering and monitoring is an important part of the online safety picture at Raynes Park High School and the governors ensure that appropriate filters and monitoring systems are in place on the school's ICT resources. Moreover, the governors have a whole school approach to online safety, which includes policies and procedures on mobile technology use in the school. Some students have access to the internet via 3G or 4G enabled devices unfiltered by the school and the school's policy on confiscation of inappropriate items will be used if it is found that such devices are being used inappropriately on the premises
- Governors will ensure compliance with the Data Protection Act and GDPR for all personal data held
- Governors will ensure that students are taught about e-Safety, for example through ICT lessons, Assemblies and RSHE lessons
- Governors are responsible for the approval of the e-Safety policy, for reviewing the effectiveness of the policy and for dealing with issues when they arise.
- Governors receive e-Safety training/awareness sessions as part of their regular cycle of meetings
- Governors will ensure the Headteacher is held accountable for implementing this policy

Roles and Responsibilities – Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the e-Safety of members of the school community and will manage the education of students and training of staff in e-Safety and awareness of potential radicalisation in students
- The Headteacher, Designated Safeguarding Lead and e-Safety coordinator will be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff, including the Headteacher
- The Headteacher and Designated Safeguarding Lead will take appropriate action if it is felt that any student of the school may be becoming radicalised
- The Education and Inspections Act 2006 empowers the Headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and

empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-Safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

Roles and Responsibilities – e-Safety Co-ordinator

- Takes day-to-day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policy and other related policies including the safe processing of personal data
- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place
- Provides training and advice for staff
- Liaises with the local authority (LA) and reports to the Headteacher and Designated Safeguarding Lead any suspicions of students who may be becoming radicalised.
- Liaises with school ICT technical staff
- Reports regularly to Senior Leadership Team/Headteacher
- Will receive training at regular update sessions and by reviewing national and local guidance documents

Roles and Responsibilities – IT Manager and IT Support Team

The network manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Appropriate filters and monitoring systems are in place and updated on a regular basis, and oversees the school's monitoring system
- The school meets the e-Safety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/e-Safety policy and guidance
- They keep up to date with the school's online safety policy and technical information in order to carry out their online safety role effectively and to inform and update others as relevant
- Users may only access the school's networks through a properly enforced password protection policy
- The Headteacher and Designated Safeguarding Lead is informed of any suspicions of students who may be becoming radicalised
- Any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.
- The Headteacher is informed of any breaches in the processing of personal data

- They receive appropriate training on a regular basis from approved trainers to support the e-Safety of all members of the school community

Roles and Responsibilities – Teaching and Support staff
Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of e-Safety matters and of the current school e-Safety policy
- They have read, understood and signed the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies
- They report any suspected misuse or problem to the e-Safety co-ordinator/ Headteacher/Designated Safeguarding Lead/Network Manager as appropriate for investigation/action/sanction
- Digital communications with students (email/virtual learning environment (VLE)/voice) are on a professional level and only carried out using official school systems
- Students understand and follow the school e-Safety policy and the student acceptable computer usage policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities. All teaching staff using the ICT rooms will be given the opportunity to use the school ICT monitor system for the designated classroom. This will allow the staff to monitor student's screens during the lesson.
- They are aware of e-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- They are aware of the e-Safety issues pertaining to email and social media usage
- They are alert to, and report to the Headteacher/Designated Safeguarding Lead, any suspicions of students who may be becoming radicalised
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- They receive e-Safety training and understand their responsibilities, as outlined in this policy. An audit of the e-safety training needs of all staff will be carried out regularly. Training will be offered as a planned programme of formal e-safety training available to all staff. All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable usage policies.

- Schools/colleges should recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School/colleges have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and should have appropriate systems in place to support and evidence this.
- Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), however schools and colleges should recognise that a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children eg victims of abuse and SEND, may be needed.

Roles and Responsibilities – Designated Safeguarding Lead

The designated person for safeguarding has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated. The DSLs is trained in e-Safety issues and will be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting
- Suspicions of radicalisation

In addition, they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required keeping children safe online.

Roles and Responsibilities – e-Safety Committee

Members of the e-Safety committee (Designated Safeguarding Lead, e-Safety Coordinator, Network Manager, Safeguarding Governor, e Safety Link Governor, Cyber Link Governor) will assist with the development of e-Safety education.

Roles and Responsibilities – Students

Students:

- Are responsible for using the school ICT systems in accordance with the student acceptable computer usage policy and agreement, which they will be expected to sign before being given access to school systems. Visiting students, will be expected to sign the visiting student acceptable computer usage agreement before access is authorised.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials, including suspicions of students who may be becoming radicalised, and know how to report such abuse

- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices including the school's policy on confiscation of inappropriate items where it relates to the use of mobile phones

- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying

- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Will understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety policy covers their actions out of school.

Roles and Responsibilities – Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

- Parents and carers will be responsible for endorsing (by signature) the student acceptable computer usage agreement

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues by providing information in a number of ways. This may include:

- Parent/Carer Evenings

- E-Safety awareness evenings

- Newsletters

- Letters

- Website/VLE

- Information about all relevant national/local e-Safety campaigns/literature

- Information about useful organisations /support services for reporting e-Safety issues (see appendix 2)

E-Safety in the Curriculum

E-safety is taught in specific areas of the curriculum but is also emphasised whenever students are using computers online. Staff always consider age-appropriateness when speaking of e-safety and will be aware of those students who may be particularly vulnerable, e.g. looked-after children or those with special needs. The school may use external resources and external visitors to assist in lessons, but appropriate members of staff will check in advance to ensure that they will enhance lessons and that materials used are appropriate for them. A planned e-Safety programme will be provided as part of ICT and L4L– this will include both the use of ICT and new technologies in school and outside school.

- Key e-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students will be helped to understand the need for the student acceptable computer usage agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students will be taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Rules for use of ICT systems/internet will be posted in all relevant rooms and displayed on log-on screens where appropriate.

In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to search the internet freely, eg using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.

It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.

The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:

- Discussing the ICT Acceptable Use Agreement and the WHS Digital Golden Rules and their implications. Reinforcing the principles via display, classroom discussion etc.

- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation

- Recognising positive use of technology by pupils.

Management of Infrastructure
The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-Safety technical requirements outlined in the acceptable computer usage policy and any relevant LA e-Safety policy and guidance

- Personal data is held and processed in compliance with the Data Protection Act and GDPR. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See the internal data security policy and code of conduct)

- There will be regular reviews and audits of the safety and security of school ICT systems

- Servers, wireless systems and cabling will be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually,

- All users will be provided with a username and password by the network manager

- The 'master/administrator' passwords for the school ICT system, used by the network manager (or other person) are also available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)

- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The school maintains and supports the managed filtering service provided by London Grid for Learning and Senso Cloud

- Any filtering issues should be reported immediately to the network manager

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data

- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users
- Agreements are signed by members of staff in possession of school provided laptops regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on laptops and other personally owned devices that may be used out of school
- The school infrastructure and individual workstations are protected by up-to-date virus software
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. See the Data Protection Policy and Staff Code of Conduct.

Filtering and Monitoring

KCSIE 2025 now encourages schools to meet specific filtering and monitoring standards and includes a new self-assessment tool from the DfE guidance Generative AI: product safety expectations. This guidance on generative artificial intelligence (AI) explains how filtering and monitoring requirements apply to the use of generative AI in education and supports schools to use generative AI safely (https://shorturl.at/5Rbsk).

Protocols on Using Digital and Video Images

- When using digital images, staff inform and educate students about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet eg on social networking sites
- If any incidents come to light about 'sexting' ie the sharing of sexual images of pupils under 18, the Designated Safeguarding Lead should be advised in the first instance
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images
- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained

Protocols on Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and in compliance with the General Data Protection Regulation which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff will ensure that they comply with the Data Protection Policy by:

- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transferring data using encryption and secure password protected devices

Protocols for Handling Electronic Communications
When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users need to be aware that email communications may be monitored
- Users will be expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable/Inappropriate Activities
Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on safeguarding and e-Safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images

- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Potential radicalisation of students

Should any serious e-Safety incidents take place, the appropriate external authorities will be informed e.g. MASH and the School's safety community police officer or, for personal data breaches, the Information Commissioner's Office (ICO).

The school will monitor the impact of the policy using:

Logs of reported incidents

Monitoring logs of internet activity (ie ISP, school network or managed service as appropriate)

Internal monitoring data for network activity

Surveys/questionnaires of students, parents/carers and staff

The policy will be reviewed by the governors annually, or more regularly, in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to e-Safety as advised by the e-Safety coordinator or others.

Social Media

Expectations

The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger

All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times

Staff use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities
- Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct, staff Acceptable Use Agreement and Social Media Policy

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, via age-appropriate sites and resources
- The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age
- The school will control pupil access to social media whilst using school-provided devices and systems on site:
  - The use of social media during school hours for personal use is only permitted for Sixth Form Students. This does not include explicit permission given by staff during appropriate activities and or lessons.
  - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), self-generated images of sexual abuse as a result of online grooming, cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- Where there is suspicion that illegal activity has taken place, the school will contact the Police

APPENDIX 1

Acts of Parliament relevant to e-Safety in schools

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment. (This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.)

Computer Misuse Act 1990 (sections 1–3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

Gain access to computer files or software without permission (eg using someone else's password to access files).

Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).

Impair the operation of a computer or program (eg caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgment. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Counter-Terrorism and Security Act 2015 (section 26)
The prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)
It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years imprisonment.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and data users must comply with important data protection principles when handling personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to cyber-bullying/bullying:

- Headteachers have the power 'to such an extent as is reasonable' to regulate the conduct of students off-site

- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

General Data Protection Regulation (GDPR)
The General Data Protection Regulation became effective in May 2018 and is legislation designed to strengthen and unify the safety and security of all data held by organisations within the European Union. In EU legislative terms, it updates and replaces the 1995 Directive. In national UK terms, it replaces the current 1998 Data Protection Act.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false, or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Obscene Publications Act 1959 and 1964
Publishing an 'obscene' article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows, or ought to know, that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Public Order Act 1986 (sections 17–29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (eg to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network.) Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as 'sexting'). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

APPENDIX 2

Useful organisations/support services for reporting e-Safety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

On-line content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Getting help/advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.

- UK Safer Internet Centre to report and remove harmful online content. https://reportharmfulcontent.com

- CEOP for advice on making a report about online abuse. https://ceop.police.uk/safety-centre/

Getting help/advice: for parents

- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk

- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 5pm, Mondays and Tuesdays on 0207 823 5430 www.kidscape.org.uk.

- *Childnet International* Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them'. Contact details are: www.childnet.com phone 020 7639 6967, email info@childnet.com.

- *UK council for child internet safety (UKCCIS)* has practical guides to help parents and others with internet safety www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.

- *Thinkuknow* has a section for parents which offers advice on protecting children from abuse online offered by the National Crime Agency's CEOP Command www.thinkuknow.co.uk/parents.

- *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. https://www.internetmatters.org

- *Let's Talk About It* provides advice for parents and carers to keep children safe from online radicalization. https://www.ltai.info/staying-safe-online/

Getting help/advice: for teachers

DFE has a telephone helpline (0207 340 7264) and an email address (counter.extremism@education.gsi.gov.uk) to enable teachers to raise concerns or questions directly with them.

- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely. https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19#safeguarding-pupils-and-teachers-online
- Department for Education (DfE) (2025) Keeping children safe in education 2025: statutory guidance for schools and colleges. [Accessed 05/08/2025]. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Generative AI: product safety expectations. https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations

UK Safer Internet Centre guidance on safe remote learning. https://swgfl.org.uk/resources/safe-

- remote-learning/

- London Grid for Learning guidance, including platform specific advice. https://national.lgfl.net/digisafe/safe-remote-learning

- *Case studies* on remote education practice are available for schools to learn from each other. https://www.gov.uk/guidance/get-help-with-remote-education

RAYNES PARK HIGH SCHOOL

Equality Impact Assessment

Policy	E Safety
EIA completed by:	Mr Phillip Nash
Contributors to EIA:	Mr Phillip Nash
Policy will affect	✓ Students ✓ Staff ✓ Governors ✓ Volunteers ✓ Visitors
Date completed:	04/12/2025

Impact analysis

- Indicate what type of impact this policy will have for each group, and explain why
- If a policy doesn't impact a group, tick the 'neutral impact' column and record this
- Remember that a policy may impact a group in multiple ways. For example, your curriculum policy may positively impact BAME students by promoting British values of mutual respect and tolerance, but negatively impact BAME students by failing to promote material that highlights a variety of cultures and ethnicities

GROUP	POSITIVE IMPACT	NEUTRAL IMPACT	NEGATIVE IMPACT	WHY WILL THE POLICY HAVE THIS EFFECT?
Example Protected characteristic	✓			Explain the impact you have recorded, and provide evidence for this, for example: ▪ Consultations ▪ Student data ▪ National data, reports, and best practice advice
Sex		✓		
Race		✓		
Religion or belief		✓		
Sexual orientation		✓		
Gender reassignment		✓		
Pregnancy or maternity		✓		
Age		✓		

Disability		✓		
Marriage or civil partnership		✓		
	Additional contextual groupings			
EAL		✓		
LAC		✓		
Families with separated parents		✓		

Outcomes

CONSULTATION AND STAKEHOLDER ENGAGEMENT
Include details of any internal or external consultation done, and its outcomes: Policy has been discussed and reviewed with the help of the head of IT, cyber security lead and the designated safeguarding lead. School governors who form part of the e-safety committee were also consulted.

FINAL DECISION ON POLICY
Please tick the appropriate decision: ☐ Remove the policy (if it's not statutory) ☐ Adapt the policy to address the equality issues you've identified ✓ Keep the policy without change