PARKSIDE MIDDLE SCHOOL

ONLINE SAFETY POLICY

Dated: October 2024

Review date: October 2026

Headteacher……

Chair of Governors……

Embrace Opportunity. Nurture Success. Inspire Futures

Parkside Middle School

Online Safety Policy

Introduction

Parkside Middle School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

Staff in schools, as well as children and young people, may be affected by online safety issues including cyberbullying and sexting incidents. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. It may have a significant impact not only on the person being bullied, but on their home and work life too. Career progression may be affected, and there have been cases where the person bullied has chosen to leave the education sector altogether. Dealing with incidents quickly and effectively is key to minimising harm in potentially highly stressful situations. Online safety, however, is about more than cyberbullying. It is about protecting one's online reputation, the managing of personal information and the responsible use of technologies, including social media.

The Governing Body will ensure that comprehensive online safety education is provided that includes support for both pupils and staff on managing personal information in online environments, and in using personal and social technologies responsibly.

Roles and Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.
The named Online Safety Lead are Mrs Jenkin. Mrs Jenkin is tasked with overseeing and managing the recording, investigation and resolution of online safety incidents.

All breaches of this policy must be reported to the Headteacher.

All breaches of this policy that may have put a child at risk must also be reported to the DSL, Mrs Jenkin.

The Governing Body will ensure that this policy will be reviewed and monitored periodically.

All staff will familiarise themselves with this online safety policy and procedures.

Staff emails that are marked 'personal' and/or 'union business' will not be read by school management without prior consent.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents:

- Safeguarding and Child Protection Policy
- Keeping Children Safe in Education
- General Data Protection (GDPR) Policy
- Health and Safety Policy
- Home–school Agreement
- Home Learning
- Behaviour for Learning and Positive Relationships Policy
- Anti-bullying Policy
- PSHCE/RSHE policies

Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Sharepoint for all official school communication to ensure everyone is protected through the traceability of communication. Multi-factor Authentication (MFA) is in use for all staff as an additional layer of security to prevent unauthorised users from accessing sensitive and confidential data. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the GDPR policy. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report to the ICT team immediately.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online content.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative).
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative).
- Adult material that breaches the Obscene Publications Act in the UK.
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation.
- Promoting hatred against any individual or group from the protected characteristics above.
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy.
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not:

- Reveal or publicise confidential or proprietary information.
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses.
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school.

- Use the school's hardware and Wi-Fi facilities for running a private business.
- Intimidate, threaten or cause harm to others.
- Access or interfere in any way with other users' accounts.
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images, such as CCTV images, are restricted to approved staff as determined by the Headteacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school, but they must be handed in to be locked away during the school day. Pupils must not use them for personal purposes within the school day. Under no circumstance should pupils use their personal mobile devices/phones to take images of:

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefits and carry out risk assessments before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the school before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff; the DSL, Mrs Jenkin or the Headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to Children's Social Care via The Family Front Door or the police.

Curriculum

Online safety is fully embedded within our curriculum. Parkside Middle School provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHCE and RSHE curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include the following areas.

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment.
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives).
- Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online.
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.
- Understanding the permanency of all online postings and conversations.
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse.

Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies.

New staff are provided with a copy of the Online Safety Policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children, based on the school premises and who will use the school's ICT system are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement.

Guidance is provided for occasional visitors, volunteers and parent/carer helpers.

Working in Partnership with Parents/Carers

Parkside Middle School works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read and discuss with each child the Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

Responding to cyberbullying incidents and reporting

- Staff should never personally engage with cyberbullying incidents. Where appropriate, they should report incidents to the nominated person and/or seek support.

- Staff should keep any records of the abuse – text, emails, voicemail, website or instant message. If appropriate, screen prints of messages or web pages could be taken and time, date and address of site should be recorded though care needs to be taken when copying certain images.

- Staff should inform the nominated person of incidents at the earliest opportunity.

- Where the perpetrator is known to be a current pupil or colleague, the majority of cases will be dealt with most effectively under the relevant school disciplinary procedure.

- Monitoring and confiscation must be appropriate and proportionate. Except in exceptional circumstances (for example, where disclosure would prejudice the conduct of a criminal investigation) parents, employees and learners will be made aware, and their consent sought, in advance of any monitoring (for example, of email or internet use) or the circumstances under which confiscation might take place. Searches without consent can only be carried out on the school premises or, if elsewhere, where the member of staff has lawful control or charge of the pupil, for example on school trips in England or in training settings. The powers only apply in England.

- Where a potential criminal offence has been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police inquiries.

- Where pupils are found to have made unfounded, malicious claims against staff members, relevant and appropriate disciplinary processes will be applied with rigour, as is the case in relation to physical assaults.

- Staff should report all incidents to the nominated person. In cases of cyberbullying, the nominated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

Responding to sexting incidents and reporting procedures

- Incidents of sexting, i.e. the production and/or sharing of sexually explicit text messages, indecent images and videos of children under the age of 18, will not be tolerated. It is an offence to possess, distribute, show and make indecent images of children and to send sexually explicit text messages. All incidents will be reported to the Police.

- If staff members receive a report of, or suspects, a sexting incident, they should refer the issue to the school's designated safeguarding lead via the school's normal child protection procedures.

- If a device is involved – it should be secured and switched off. Staff should not search the device if this will cause further embarrassment/distress to the pupil involved, unless there is clear evidence to suggest there is an immediate problem.

- The designated safeguarding lead must treat all sexting incidents as a child protection issue, and apply judgement, in a consistent manner, to decide on a response to each case. Further advice on issues to consider when making a judgement is available at http://www.saferinternet.org.uk/

- A risk assessment should be carried out, and necessary safeguards put in place for the pupil (e.g. they might require counselling or further support).

- Sanctions will be enforced if any member/s of the school community breaches school policies relating to sexting. If the images or text messages used are considered illegal, this may involve making referrals to the police. It there are concerns that the child is at risk, a referral to children's social care is likely to be necessary.

- All sexting incidents must be recorded by the school's designated safeguarding lead, regardless of whether the incident leads to a referral to external agencies.

Action by school: Inappropriate Use of Social Networking Sites

Following a report of inappropriate use of social networking sites, the nominated person will take the following action:

- Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed.

- If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. The material posted may breach the service provider's terms and conditions of use and can then be removed.

- In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.

- Before the nominated person contacts a service provider, he or she will check the location of the material – for example by taking a screen capture of the material that includes the URL or web address. If the nominated person is requesting that the service provider takes down

material that is not illegal, he or she will be clear how it contravenes the site's terms and conditions.

Where the alleged 'offender' is a member of the school community (including parents/carers) the school will:

- deal with harassment and bullying under the relevant school procedure
- take care to make an informed evaluation of the severity of the incident
- deliver appropriate and consistent sanctions
- provide full support to the staff member(s) affected

The Governing Body recognises its legal duty to protect staff from unlawful harassment as well as mental and physical injury at work.

In cases of potentially criminal content, the nominated person will consider whether the police should be involved, following appropriate liaison with staff, and parents where necessary.

Records, monitoring and review

Parkside Middle School recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported, and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Staff should record any concerns via My Concern or Form 1.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

This policy operates in conjunction with the following school policies:

- Safeguarding and Child Protection Policy
- General Data Protection Policy
- CCTV Policy
- Quality of Education Policy

Date of policy: October 2024

Review date: October 2026

APPENDIX 1

USEFUL INFORMATION FOR NOMINATED ONLINE SAFETY LEADS

Useful information for the nominated online safety lead including a list of service providers is set out below.

Mobile Phones

All UK mobile phone providers have malicious, or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. They can help you to change the number of the person being bullied if necessary. It is not always possible for operators to block numbers from contacting the person being bullied, but many phones, such as iPhones allow users to block phone numbers.

If the victim wants the perpetrator prosecuted contact the police. If a bully is making direct threats which constitute a real danger, phone 999. If there isn't an immediate danger, then contact the non-emergency number 101. The mobile provider can work closely with the police and can usually trace malicious calls for them.

Contact details for service providers:

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	202 (pay monthly) 4445 (pay as you go)	0344 8090 222	0344 809 0202
Vodafone	191	0333 3040 191	0333 3040 191
3	333	0333 338 1001	0333 338 1001
EE	150	0800 956 6000	0800 956 6000
BT	0800 023 2023	0800 023 2023	0800 023 2023
Tesco Mobile	4455	0345 301 4455	0345 301 4455
Sky Mobile	150		

Contact details for social networking sites:

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools. Advice can be found here http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/safety-tools-on-online-services

Facebook Read Facebook's Terms of Use Report to Facebook Facebook Safety Centre	**YouTube** Read YouTube's Terms of Use Report to YouTube YouTube Safety Centre
Instagram Read Instagram's Terms of Use Report to Instagram Instagram Safety Checklist	**X** Read X's Terms of Use Reporting to X X Safety Centre
TikTok Read TikTok's Terms of Use Report to TikTok TikTok Safety Centre	**Snapchat** Read Snapchat's Terms of Use Report to Snapchat Snapchat Safety Centre
WhatsApp Read WhatsApp's Terms of Use Report to WhatsApp WhatsApp Safety and Security	

Video and photo hosting sites

YouTube: Logged in YouTube members can report inappropriate content at: http://support.google.com/youtube/bin/answer.py?hl=en&answer=95403

Flickr: Reports can be made via the `Report Abuse' link which appears at the bottom of each page. Logged in members can use the `flag this photo' link to report individual pictures. www.flickr.com/guidelines.gne

Instant Messenger

It is good practice for Instant Messenger (IM) providers to have visible and easy-to-access reporting features on their services. Instant Messenger providers can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations, and most IM providers allow the user to record all messages.

Contacts details for some IM providers:

WhatsApp: There are details in the FAQs section on blocking other users (http://www.whatsapp.com/faq/en/general/21242423). There isn't a service to report abuse, but details can be emailed to support@whatsapp.com.

Skype: https://support.skype.com/en/faq/FA10001/how-do-i-report-abuse-by-someone-in-skype

Messenger: Reporting Abuse | Messenger Help Centre (facebook.com)

iMessage: Block, filter, and report messages on iPhone – Apple Support (UK)

Chatrooms, individual website owners/forums, message board hosts

It is good practice for chatroom providers to have a clear and prominent reporting mechanism to enable the user to contact the service provider. Users that abuse the service can have their account deleted. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use.

Live Streaming

YouNow: safety information and details of how to contact a moderator available at - https://www.younow.com/policy/en/trust

Vimeo: Vimeo OTT Terms of Service and Policies – Vimeo Help Center

APPENDIX 2

How to Stay 'Cyber safe' – Dos and Don'ts for school staff

Do

- Be aware of your online reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available online information. Type your name into various search engines to see what information there is about you on the internet. Remember, the internet never forgets.

- Keep passwords secret and protect access to accounts – always log off from any device that you have been using, even if you are only stepping out of the room for a moment and ensure that all phones and tablet devices are secured with a passcode.

- Regularly review your privacy settings on social media sites and your devices (mobile phone, tablet, laptop etc.).

- Discuss expectations with friends – are you happy to be tagged in photos.

- Be aware that, increasingly, individuals are being held to account in the courts for the things they say on social networking sites.

- Keep personal phone numbers private and don't use your own mobile phones to contact pupils or parents.

- Use a school mobile phone when on a school trip.

- Keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible (Note: you can find out your IMEI number by typing *#06# on your handset – the number will be displayed on the screen).

- Ensure that school rules regarding the use of technologies are consistently enforced.

- Report any incident to the appropriate member of staff in a timely manner.

- Keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material (staff need to be aware that taking a screenshot of content which is potentially illegal could result in staff committing a criminal offence) including the URL or web address.

- Use school email address only for work purposes.

- Be aware that if you access any personal web-based email accounts via the school network, that these may be subject to the school's internet protocol which could include monitoring and surveillance.

- Request assurances from management that any emails marked 'personal' and/or 'union business' will not be read without your prior consent.

- Raise genuine concerns about your school or certain members of staff using your employer's whistle blowing or grievance procedure.

Don't

- Post information and photos about yourself, or school-related matters, publicly that you wouldn't want employers, colleagues, pupils or parents to see.
- Befriend pupils or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents or ex-pupils).
- Personally retaliate to any incident, bullying messages.
- Criticise your school, pupils or pupils' parents online.

More helpful tips are available from the UK Safer Internet Centre at www.saferinternet.org.uk under 'Advice and Resources'.

APPENDIX 3