PARKSIDE MIDDLE SCHOOL
ONLINE SAFETY POLICY

Dated: October 2022

Review date: October 2024

Headteacher……

Chair of Governors……

Parkside Middle School

Online Safety Policy

Introduction

Staff in schools, as well as children and young people, may be affected by E-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. E-safety, however, is about more than cyberbullying. It is about protecting one's on-line reputation, the managing of personal information and the responsible use of technologies, including social media.

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

Roles and Responsibilities

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

The Headteacher will ensure that the school has a nominated person as E-safety Lead (a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of E-safety incidents).

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

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

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, e-mails, voice mail, web site 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 e-mail 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.

APPENDIX 1

USEFUL INFORMATION FOR NOMINATED E-SAFETY LEADS

Useful information for the nominated E-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 particular 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 (Orange and T Mobile)	150	0800 956 6000	0800 956 6000
Virgin	789	0345 6000 789	0345 6000 789
BT	150	01793 596931	01793 596931

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 rules Report to Facebook Facebook Safety Centre	**YouTube** Read YouTube's rules Report to YouTube YouTube Safety Centre
Instagram Read Instagram's rules Report to Instagram Instagram Safety Centre	**Twitter** Read Twitter's rules Reporting to Twitter
Vine Read Vine's rules Contacting Vine and reporting	**Kik Messenger** Read Kik's rules Reporting to Kik Kik Help Centre
Ask.fm Read Ask.fm's 'terms of service' Read Ask.fm's safety tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.	**Tumblr** Read Tumblr's rules Report to Tumblr by email If you email Tumblr take a screen shot as evidence and attach it to your email

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.

Snapchat: safety information and reporting options are available at - https://support.snapchat.com/ca/abuse

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

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

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

Periscope: details of how to report inappropriate content are available at https://help.periscope.tv/customer/en/portal/articles/2064647-what-if-i-find-inappropriate-content- and the terms of service are available at https://www.periscope.tv/tos

APPENDIX 2

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

Do

- be aware of your on-line 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 on-line 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 e-mail address only for work purposes.

- be aware that if you access any personal web-based e-mail 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 e-mails 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


STAY SAFE ON SOCIAL NETWORKING SITES
Never say anything you would not be prepared to say in any other forum (particularly about other people).
Don't criticise your school, pupils or pupils' parents online.
If you have a genuine concern about your school, or certain members of staff, raise your concerns using your employer's whistle blowing or grievance procedures.
Be aware that increasingly, individuals are being held to account in the courts for the things they say on social networking sites.
Be careful about befriending pupils and ex-pupils online.
Always save evidence of any offending messages about you or your colleagues.
Don't retaliate online to bullying messages.