E-Safety Policy:
Parkgate Primary School 2022-2023

1. Introduction:

Parkgate Primary School	Designated Safeguarding Lead (DSL) team	Mrs Zoe Richards (DSL) Mrs Zoe Brown (Deputy DSL) Mr Ben Henley (Deputy DSL)
	Online-safety Lead	Mr Ben Henley
	Online-safety / safeguarding link Governor/Board Member	Mrs Carol Blair
	Network manager / other technical support	Mr Andrew Wilks
	Date this policy was reviewed and by whom	September 2022 by Carol Blair
	Date of next review and by whom	August 2023

Our pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. This presents many positive and exciting opportunities, but also challenges and risks.

The use of the latest technology is actively encouraged at Parkgate but with this comes a responsibility to protect both pupils and the school from abuse of the system.

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

Overview – Aims

This policy aims to:

- Set out expectations for all Parkgate community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and

- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

Scope

This policy applies to all members of the Parkgate community (including staff, the proprietor, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported. (At Parkgate School the Headteacher is also the DSL)
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Children's Safeguarding Partnership in Coventry guidance
- Liaise with the designated safeguarding lead and online safety coordinator on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL, LGB and senior management team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure the LGB is regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure all remote learning policies are kept up to date
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead

The DSL at Parkgate will take lead responsibility for Child Protection and Safeguarding (including online safety).

The Online Safety Lead will work alongside the DSL to ensure an effective approach within the school.

The Online Safety Lead and DSL will meet on a regular basis.

Key Responsibilities;

- "Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, LGB and senior management team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the headteacher
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with the senior management team and the designated advisory board member for child protection to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with the Proprietor and ensure staff are aware.
- Ensure the 2021 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation.
    - Keep all remote learning policies up to date.

Local Governing Body

Key responsibilities:

- Approve this policy and strategy and subsequently review its effectiveness.
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for child protection and safeguarding (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at senior management meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; senior management team and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school

- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated in line with advice from the Children's Safeguarding Partnership in Surrey. Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.
- Ensure appropriate filters and appropriate monitoring systems are in place.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.
- Consider a whole school approach to online safety with a clear policy on the use of mobile technology.

All Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for Senior management team and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff code of conduct
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL/OSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, including the remote learning responsible user agreement for pupils, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Follow the remote learning policy and teacher protocols during any part or full school closure

PSHE Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ Relationships Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and Relationships Education.

Computing Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements, including remote learning agreements.

Network Support Specialist

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior management team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safeguarding lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy, including the remote learning responsible use policy for pupils and review this annually

- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies (including remote learning policies) cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents

Key responsibilities:

- Read and promote the school's parental acceptable use policy (AUP), Including remote learning policies and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Education and the curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE and Relationships Education
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Parkgate School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to focus on the key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

We follow the 'Education for a Connected World' framework which helps to equip children and young people for digital life. The 8 themes are also integrated into our termly assembly plans.

We follow the 'Be Internet Awesome' framework for delivering Online Safety to children.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety coordinator / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

The school's procedures for dealing with online-safety are mostly detailed in the following policies (primarily in the first key document):

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)

Parkgate School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

System security

Systems within Parkgate are managed by 'The Futures Trust'

Monitoring

The school and The Futures Trust reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate disciplinary action will be taken.

Property

Pupils and staff should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to a member of office staff.

Viruses

Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

System Security

- All computers and laptops are password protected. Passwords are changed on a regular basis.
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.

- Do not make deliberate attempts to disrupt or damage the school network, any device attached to it or any data stored on it or transmitted across.
- Do not alter school hardware in any way.
- Do not knowingly misuse headphones or any external devices e.g. printers
- Do not eat or drink while using the computer.
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data.

Leaving workstations

If a person leaves their workstation for any period of time they should log out of their workstation or lock their screen.

INTERNET

The School recognises the benefits to using the Internet in an educational environment. The Internet facility is provided for school related activities only. The school monitors the use of the Internet.

The school internet system has a filtering and monitoring system run CensorNet and RADAR which monitors and filters all website access against preset policies. Any inappropriate material, whether it be sexual, violent, extremist or illegal in nature will be blocked and the System Administrator alerted, who will in turn alert the school Designated Safeguarding Lead/ Online Safety Lead, as to the inappropriate material being accessed.

Viewing, retrieving or downloading of any material that the school considers inappropriate will result in appropriate disciplinary action.

Good practice guide for staff, pupils and parents

Staff

Staff Personal Safety

It is vitally important that staff are careful about content that they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages.

Staff need to ensure that films or other material shown to children are age-appropriate.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher.

Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school branding (uniform).
- Staff must not form online friendships with pupils and parents.
- Staff must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Staff will be required to attend an annual internet safety course and ensure that they pass this information on to the children in their care.
- Staff should use their school email account for all school-related communications.
- Staff to be aware of the various members of staff responsible for Safeguarding issues
- Staff members should refer to the Staff Code of Conduct for more detailed information.

Pupils

- The school will organise internet safety lessons on a termly basis.
- Pupils must not play with or remove any cables etc that are attached to a school computer.
- Pupils will be taught how to stay safe when working online at school and at home.
- Pupils must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Pupils must not post anything on any online site that can be constructed to have an adverse impact on the school's reputation.
- Pupils must not post photos of video related to the school on any internet sites including pupils, staff, parents or the school branding (uniform).
- Pupils should never reveal their full name, any address or contact details, any school or network user ID or password online, even if communicating with known acquaintances.
- Pupils should be aware that the potential exists for predators to remain entirely anonymous and easily pose as someone else.
- Pupils should employ a healthy mistrust of anyone that they "meet" online unless their identity can be verified.
- The use of chat rooms and social networking sites are not permitted in school.
- Do not arrange to meet anyone you have met on the internet - people are not always who they say they are.

Visit and explore the Cyber Cafe for your age group at http://www.thinkyouknow.co.uk for more information about how to stay safe when working online.

Parents

- Parents will be invited to an annual e-safety evening run by an external presenter which will consist of advice and useful tips to help support them in ensuring their child's computer and internet safety at home.
- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

A link to our free online safety magazine for schools can be found in the parents section on the school website.

You can find out more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to children about e-safety at;

The UK Safer Internet Centre website

http://www.saferinternet.org.uk

CEOP's Thinkuknow website

http://www.thinkuknow.co.uk
http://www.thinkyouknow.co.uk/parents

Internet Matters

http://www.internetmatters.org

Childnet

http://www.childnet.com/sns

NSPCC

http://www.nspcc.org.uk/onlinesafety

Parent Zone

http://www.parentzone.org.uk

Ask About Games (where families make sense of video games)

http://www.askaboutgames.com

Inappropriate Behaviour

Bullying of another person will be treated with the highest severity.

Online, Cyber Bullying

- Lessons concerning cyber bullying to be carried out termly through the computing and PSHE curriculum.
- By cyber bullying, the School is referring to: bullying by email, messages, images, calls or other electronic communication.
- Use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites (including social networking sites).
- Hijacking or hacking email accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms or on instant messaging services.
- The use of Social Media for the use of bullying, grooming, abuse and radicalisation.

Pupils should be aware that cyber bullying is generally criminal in character and that English law does apply. The School will endeavour to resolve all matters using the School's Behaviour Policy without Police involvement but parents of victims do have the right to seek Police intervention. This will be closely linked to the School's Anti-Bullying Policy and Parkgate's Child Protection and Safeguarding Policy which can be read separately or in conjunction with this policy.

Have concerns as a parent

There's lots of information and advice on the http://www.thinkyouknow.co.uk site to keep your child safe and access support.

Having a calm and open conversation is one way for you and your child to explore what is happening in an honest and supportive way.

Discuss your concerns with someone you trust, for example a friend, partner or the school.

You can also talk to a professional at the NSPCC helpline on 0808 800 5000.

Talking about it will help decide the best action to take to ensure your child is safe.

TO MAKE A REPORT

If you are concerned about online grooming or sexual behaviour online you can contact CEOP: http://www.ceop.police.uk or alternatively you can click on the 'Report Abuse' button located at http://www.thinkyouknow.co.uk.
If you stumble across criminal sexual or obscene content on the internet you should report it to the Internet Watch Foundation: http://www.iwf.org.uk.

You can also report directly to your local police force.

If you think your child is in immediate danger call 999.

Email

Personal use

Email is provided for school related purposes only. The school monitors the use of email and disciplinary action may be taken if inappropriate uses of personal emails are discovered.

Status

Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. Pupils and staff should not include anything in an email that is not appropriate to be published generally. Any email message which is abusive, discriminatory on grounds of sex, race, disability, sexual orientation or religious belief, or defamatory is not permitted.

Privacy

All files and emails on the system are property of the School. As such, system administrators and staff have the right to access them if required.

Copyright

You should respect copyright. Breaking copyright laws occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner. This includes the copying of music files and CDs.

The School purchases appropriate licences where required.

Photography – Digital Images and Video

The word photography is used in this policy to include traditional photographs and digital images of any kind, still or moving.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Photography and video are familiar features of life, playing a significant role in commerce, entertainment and communication; it is commonplace in our homes and it is an important element of school life.

At Parkgate we feel it is vital that achievements are recognised and that pupils feel valued, proud and happy. Photography is a useful tool within school and it is employed routinely in many ways, for example; record keeping, displays, special events, teachers' lessons and the children's own work.

On occasions photos are also used for the Press, school website, school facebook page and other promotional purposes.

Children will only be named in photographs that are displayed within the school. We will not provide children's full names for any other purpose unless special parental consent has been received.

We are, however, sensitive to the wishes and rights of parents who may not wish their children to be photographed and who may have concerns about the use of such images.

Parents are requested to update preferences relating to use of digital images annually.

Social Media

Parkgate School works on the principle that if we don't manage our social media reputation then someone else will.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Staff, pupils' and parents' social media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school.

Pupils and parents are not allowed* to be 'friends' with or make a friend request** to any staff, volunteers and contractors or otherwise communicate via social media.

Pupils and parents are discouraged from 'following' staff, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

Use of mobile phones

The following rules apply for the use of personal mobile phones;

Pupils

- Pupils are not permitted to bring mobile phones, smartwatches or personally owned devices into school.
- Pupils in Year 5 and Year 6 who have been given permission by the Headteacher to walk to and from school must sign in their mobile phones at the school office when they arrive in the morning for safe-keeping in a locked location during school hours.
- Pupils must sign out their mobile at the end of the day just before leaving the school premises.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with school policy.

Staff

- The school accepts that employees will bring their mobile phones to work.
- Mobile phones and personally owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- Employees are not permitted to make/receive calls/texts during lessons or formal school time or use recording equipment on their mobile phones or personal devices to take photographs/videos of children.
- Staff use of mobile phones during the school day will normally be limited to the morning/lunch break and after school.
- Mobile phones should be switched off (or silent) and left in a safe place during lesson times. Staff should use phones in designated areas. The designated area is the Staff Room. If a private call needs to be made then a request for a room can be made to the Headteacher.
- Mobile phones are not permitted in areas where children are present.
- In the event that an employee has a particular reason for a specified period of time, they may request via the Headteacher that they leave their phone on during working hours.
- If a staff member breaches the school policy then disciplinary action may be taken as appropriate.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Mobile phones should not be used in a space where children are present unless the School phone is being used for a medical reason or the teacher is on a school trip.

Acceptable Use Policies

Please see Appendix

Remote Learning Policies and Agreements for part or full COVID-19 School Closure

Remote Learning at Parkgate - Teacher Protocols

Remote learning at Parkgate School during any enforced part or full school closure or while pupils are self isolating will ensure that we stay connected with the school community. It will not only allow the learning process to continue but will also provide important support for pupil well being.

The platform that should be used for all remote sessions is Seesaw or Showbie (dependant on child's year group) Details about each remote learning session and any support material/s can be posted within the platform. It is important to get the pupils into the habit of opening up Seesaw or Showbie every morning so they can keep up to date with posted lessons and activities that they have been asked to complete and then hand in.

Seesaw or Showbie can be used for:

- Class teaching
- Review and Feedback
- Pastoral check-ins
- Group Reading Sessions
- Assemblies

To create a safe environment for our pupils when engaging in remote sessions, there are several things that a teacher should consider.

- We must have consent from parents/carers to access the remote learning sessions. Consent will be gained by the parents/carers completing the 'Parent Consent Form for Remote Learning Sessions'.
- Pupils will also be required to sign a 'Remote Learning Responsible Use Agreement'.
- Teachers should familiarise themselves with the functions of Seesaw or Showbie.
- Each class teacher must share their proposed remote learning timetables with the Headteacher.
- Teachers need to consider and be sensitive to the needs of individual pupils, and children who may be sensitive to certain topics or issues that may arise during the remote sessions.

Essential Rules

- Keep a record of attendance.
- Teachers should communicate with the Headteacher or DSL should any interactions not be appropriate or conducive to learning.
- The School's Safeguarding and Staff Code of Conduct must be adhered to at all times, this includes sessions that may need to be delivered from home.

Remote Learning Responsible User Agreement for Pupils

Remote learning at Parkgate School during any enforced part or full school closure or if a pupil is self isolating will ensure that we stay connected as a school community. It will not only allow the learning process to continue but will also provide important support for pupil well being.

In the event of a return to remote learning you will receive a class timetable indicating the time of each remote learning session. You will be able to access the sessions through your secure wwsch.net account and the Google Meet and Classroom apps.

Rules

- I will only use technology for school purposes as directed by my teacher.
- I will only use technology when there is an adult in the house and they know I am using it.
- I will not reveal my passwords to anyone.
- I will be responsible for my behaviour and actions when using technology, this includes the resources I access and the language I use.
- I will make sure that all my communication with pupils, teachers and others using technology is responsible and sensible.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across such material I will report it immediately to my teacher or my parents.
- I understand that when using Seesaw or Showbie and other applications provided by the school that my use is monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents may be contacted.

Guidelines

When using Seesaw or Showbie, remember that this is an extension of the classroom and you should conduct yourself as you would in the classroom. This includes:

- Complete and hand in all work on time
- Have all the equipment that you need for each session nearby such as your pencil case, textbook and exercise books
- Remain attentive during sessions
- Interact patiently and respectfully with your teachers and peers
- Provide feedback to teachers about your experiences and any relevant suggestions

Parental Consent Form for Remote Learning Sessions

Remote learning at Parkgate School during any enforced part or full school closure, or if a pupil is self isolating will ensure that we stay connected as a school community. It will not only allow the learning process to continue but will also provide important support for pupil well being.

In order to deliver remote learning we must receive parental permission before a pupil is able to take part.

Pupils are expected to read and discuss the 'Remote Learning Responsible Use Agreement' with you, and then follow the terms of the policy. Any concerns or queries can be discussed with the Headteacher.

To facilitate remote learning during part or full school closure or if a child is self isolating, parents should support by:

- Ensuring your child attends each remote learning session, completes and hands in any work set on time
- Provide your child with a workspace with a neutral background that is quiet, safe and free from distractions with an adult nearby if necessary
- Parents may not record, share or comment on public forums about individual teachers.

E-Safety Note - Please be aware any online interaction by your child outside of Seesaw or Showbie is not monitored by the school and is therefore your responsibility.

By signing this form, you give permission for your child to attend remote learning sessions with Parkgate staff, acknowledge that you have shared the 'Pupil Remote Learning Responsible Use Agreement' and discussed remote learning with your child. It is vital that your child agrees to follow the rules.

We are here to support you every step of the way so please do make contact with either the class teacher or a member of the senior management team if you have any further questions or need any technical support. Staff members can be contacted during school hours via Seesaw or Showbie.

If you find that you do not have enough devices at home for your child/ren to take part in the remote learning sessions please do get in contact with the school office. We have a Chromebook Loan Scheme in place and will do our very best to accommodate any request.

Appendix 1: acceptable use agreement (pupils and parents/carers)

Our School E-Safety Rules KS1

All pupils use ICT including Internet access as an essential part of learning. Please read these with your child so that you understand and agree our e-safety rules.
E-Safety Rules at Parkgate Primary School **Think then click!** We can send and open emails together. We can search the internet with an adult. We always ask if we get lost on the internet. We can write polite and friendly emails to people that we know. We can click on the buttons and links when we know what they do.

Parents and children should also be aware that to keep children safe in school, the school has installed on its system '***Policy Central***' forensic software. This software monitors what is being accessed.

Pupil's Agreement

- I have read and I understand the school E-Safety Rules.
- I will use the computer, network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.
- I will use them only with a teacher's permission
- Only access appropriate websites
- I will not share my password with others or log in to the school's network using someone else's details
- I will not give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer

I agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

Signed: **Date:**

Parent's Consent for Internet Access

I have read and understood the school E-Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: **Print name:** **Date:**

Our School E-Safety Rules – KS2

All pupils use ICT including Internet access as an essential part of learning. Please read these with your child so that you understand and agree our e-safety rules.

E-Safety Rules at Parkgate Primary School

We ask permission before using the Internet.

We only use websites that an adult has chosen.

We tell an adult if we see anything we are uncomfortable with.

We immediately close any webpage we not sure about.

We only e-mail people an adult has approved.

We send e-mails that are polite and friendly.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.

We do not open e-mails sent by anyone we don't know.

We do not use Internet chat rooms.

We do not bring to school downloaded information on flash drives for use in school.

We do not access MSN or social network sites at school.

Parents and children should also be aware that under the City Councils Policy to keep children safe in school, that the school has installed on its system '***Policy Central***' forensic software. This software monitors what is being accessed.

Pupil's Agreement

- I have read and I understand the school E-Safety Rules.
- I will use the computer, network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: **Date:**

Parent's Consent for Internet Access

I have read and understood the school E-Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: **Print name:** **Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:
Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
Use them in any way which could harm the school's reputation
Access social networking sites or chat rooms
Use any improper language when communicating online, including in emails or other messaging services
Install any unauthorised software
Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
I agree that the school will monitor the websites I visit.
I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff	
Online safety training needs audit Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident