Online Safety

RHODES AVENUE PRIMARY SCHOOL

Approved by:	Full Governing Body	**Date:**	September 2022
Last reviewed on:	Spring 2019		
Next review due by:			

Contents

RHODES AVENUE PRIMARY SCHOOL

Online-Safety Policy
September 2022

By framing this policy Rhodes Avenue Primary School (hereafter referred to as 'the school') acknowledges it duty and responsibility to adhere to the statutory guidance outlined in the Department for Education's *Keeping Children Safe in Education* (KCSIE) 2022.

The school also acknowledges its legal duties under the *Equality Act 2010* and its duties, in respect of safeguarding and in respect of pupils with special educational needs (SEND).

This policy should not be viewed in isolation, the principles and practicalities of this document also run through other school policies; namely the Safeguarding and Child Protection Procedures Policy, the Behaviour for Learning, Anti-Bullying, Social Media and Prevent policies.

Context

All users need to be aware of the range of risks associated with the use of internet and social media technologies. The school embraces its responsibility to educate its pupils on E- Safety; teaching the appropriate behaviours and critical thinking skills to enable pupils to remain safe when using the internet and related technologies, in and beyond the context of the classroom and to ensure pupils are aware of potential legal risks. KCSIE 2022 Aoppendix 5 para 143.
Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. The school holds personal data on learners, staff and other people to help them conduct their day-to- day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in adverse media coverage, and potentially damage the reputation of the school.

Aims

The aims of this policy are to:

- Set out the key principles expected of all members of the school community regarding online behaviour, attitudes and activities and use of digital technology;

- 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;
  - 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;
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope

This policy applies to all members of the school community (including staff, governors, volunteers, contractors, students/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.

Policy

At Rhodes Avenue Primary we ensure that children are safeguarded from potentially harmful and inappropriate online material. Our effective whole school approach to online safety empowers us to protect and educate our pupil, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

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

contact: being subjected to harmful online interaction with other users; for example: Child on Child Abuse, Peer Pressure, Commercial advertising and Adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;

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

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. Referrals can be made to the Anti-Phishing Working Group (https://apwg.org/). KCSIE 2022 Appendix 5 para 134-136.

Governing bodies will ensure online safety is a running and interrelated theme whilst devising and implementing our whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement. KCSIE 2022 Appendix 5 para 136.

Remote education

The following guidance can be read in conjunction with our Online Safety policy. Further information on how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and Providing remote education: guidance for schools - GOV.UK (www.gov.uk). The NSPCC also provide helpful advice - Undertaking remote teaching safely.

Rhodes Avenue Primary are in regular contact with parents and carers. Those communications are used to reinforce the importance of children being safe online and parents and carers find it helpful to understand what systems Rhodes Avenue Primary uses to filter and monitor online use. Rhodes Avenue Primary is aware that it will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from our school their child is going to be interacting with online. KCSIE 2022 Appendix 5 para 139-140

Filtering and monitoring

Rhodes Avenue Primary's governing body is aware of its responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, our governing body does all that they reasonably can to limit children's exposure to the above risks from the school's IT system. As part of this process, Rhodes Avenue Primary's governing body ensures that they have appropriate filtering and monitoring systems in place and regularly review their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Rhodes Avenue Primary's Governing body also considers the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

The appropriateness of our filtering and monitoring systems are managed by our ITC technical support officer and will be informed in part, by the risk assessment required by the Prevent Duty. Rhodes Avenue Primary has relevant risk assessments in place to monitor the PREVENT Duty. KCSIE 2022 Appendix 5 para 140-141

Actions where there are concerns about a child

Online safety concerns are no different to any other safeguarding concern.

Bullying

Online bullying is treated like any other form of bullying and the school's bullying policy will be followed for online bullying, which may also be referred to as cyberbullying.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, Rhodes Avenue Primary's designated safeguarding lead (or a deputy), will consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that **Cyber Choices** does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety KCSIE 2022 Annex B Page 143

Additional advice can be found at: Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre - NCSC.GOV.UK.

Youth Produced Sexual Imagery (Sexting)

1. A Definition

Many professionals consider sexting to be 'sending or posting sexually suggestive images via mobile technology or over the internet. Creating and sharing sexual photographs and video of under-18s is illegal. Whilst professionals refer to this behaviour as 'sexting' there is no clear definition of 'sexting'. On this basis the UK Council for Child Internet Safety(UKCCIS) has introduced the phrase 'youth produced sexual imagery' to ensure clarity about the issues their advice addresses.

Youth produced sexual imagery best describes 'sexting' because:

- Youth produced' includes young people sharing images that they, or another young person have created themselves;
- 'Sexual' is clearer than 'indecent'. A judgement of whether something is 'decent' is both a value judgement and dependent on context;
- 'Imagery' covers both still photographs and videos.

The understanding of children taking or sharing youth produced imagery is likely to be influenced by the age and ability of the children involved. In all likelihood children who create youth produced sexual imagery may be the outcome of age appropriate curiosity, risk taking behaviour or simply naivety as opposed to sexual intent. Some common examples may be sending pictures of their genitals to their friends as a dare or taking a photo of another child changing for P.E. The DSL will be required to use their professional judgement to consider the specific context and the children involved but nevertheless youth produced sexual imagery within or outside the school will be potentially seen as an indicative of a wider safeguarding or child protection concern.

The school follows the UKCCIS (https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis) guidance on 'youth produced sexual imagery' in schools:

- Report it to your DSL immediately;
- Never view, download or share the imagery yourself, or ask a child to share or download – this is illegal;
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL; Do not delete the imagery or ask the young person to delete it;
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL;
- Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers;
- Do not say or do anything to blame or shame any young people involved;
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

The school's safeguarding policies will also outline codes of practice to be followed.

KCSIE 's (September 2022) statutory guidance states that all schools should have an effective child protection policy and that the school's approach to youth produced sexual imagery should be reflected in the policy. All incidents involving youth produced sexual imagery should be responded to in line with the Safeguarding and Child Protection and Procedures Policy.

Misuse of School Technology (Devices/Systems/Networks or Platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are outlined in the school's *Acceptable Use Policy* as well as in this document.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Managing the school’s Online Reputation

The school works on the principle that if we don’t manage our social media reputation, someone else might. Online Reputation Management (ORM) is about understanding and managing our digital footprint. Few parents will apply for a school place without first ‘googling’ the school, and the Ofsted pre-inspection check includes monitoring what is being said online (e.g. Mumsnet).

The school believes that by a having a prepared clear communication strategy - being clear how a school will counter, weaken or eliminate any negative material but above all, by promoting positive news about the school - in place before any potentially damaging stories are published will reduce potential negative impact on the school. In essence, all staff, pupils and parents need to know how they are expected to behave online.

A strong online presence is about much more than reacting to bad news – it can be a highly effective strategy for engaging and connecting with prospective and current parents, pupils, partners and the community. 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.

The Headteacher is responsible for managing our Twitter account and the Deputy Head oversees the website.

1. Strategies

Researching what is being posted about our school:

- Google Alerts (google.com/alerts) it is a way of keeping track of news about our school without having to search every day. Alerts can be set up - alerts for any word, phrase or name - and can receive an e-mail whenever there is new activity using those words. The school can limit the time and amount of alerts it receives and set all alerts to be combined into one weekly digest.

- Hootsuite (hootsuite.com) is a tool for managing all school social-media accounts in one place and can also send notifications whenever certain keywords are mentioned on social media.

- There are also professional services that charge to support schools. The SWGfL Alerts tool (boost.swgfl.org.uk). It is a ‘digital ear to the ground’ that suggests whether a posting is positive or negative, and supporting any associated actions.

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the Headteacher will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals’ Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

2. Managing Negative Content

If the school locates any negative comments online, there are a number of direct or indirect responses it can make. A direct response would be posting a reply to a parent who shared negative comments online. One response could be for example:

"We notice you posted this online. We'd really welcome an official complaint, here is our complaints procedure."

An indirect comment may refer to the general topic and explain the school's position without referencing the original comment (on the same or different medium).

The school will always address caution when assessing negative comments online. We will not respond online immediately, but take time to consider a response and to seek advice.

All/any allegations (online or offline) will be managed in accordance with school procedure; it's important that all staff understand, not respond and know who to contact.

3. Communicating the message we want our community to hear

The school believes that the best approach is to develop a strong, authentic and trusted online presence that can outweigh any negative content. The school website is at the core of our communications strategy, with all other tools and resources pointing users towards it.

4. Analysing our website

The school uses *Google Analytics* (analytics.google.com) which helps it to track:

What content interests' users:
- popular pages;
- search terms;
- time spent on each page;

What page/content has not been viewed in two years, is it worth keeping;
Who our users are?;
Where users come from (e.g. Facebook or Twitter);
What device they are using (e.g. PC, mobile phone).

By reviewing our web visits we can tailor our website to support the needs of our community and ensure that it is a portal that communicates clearly to all visitors.

5. Photographs and Permissions

We ensure that we have written parental/carer permission for the uploading of photographs, images or music. Material must be copyright free or licenced for educational use. See Appendix for parental guidance.

Social Media Strategy

The school will manage social media accounts through designated staff – Headteacher/Deputy and Technical Support - knowing passwords and account details. Staff with personal social media accounts will not access school media accounts using their devices for security reasons and to avoid posting updates to the wrong account.

The school will:

use a dedicated school e-mail account to register social media accounts;

not reply to positive nor negative comments (the school may acknowledge someone who posts a negative opinion and if appropriate may invite them into school to discuss their concerns);

not enter into an argument online;

'unfriend' any troll who uses targeted systematic abuse against the school community;

remove objectionable comments;

report any user to the social network/contact the police /law enforcement if comments are significantly threatening or specific;

set rules around language and tone.

School-safe video-sharing platform

YouTube has many educational videos available for staff to incorporate in lessons but there are many inappropriate videos available online and it is a challenge to filter them and still retain access to those you want to see. The Autoplay function can promote opportunities for tenuously related videos to be played after the original choice. If a video leads into a highly inappropriate one, staff may be associated with it in viewers' minds and staff may have no control over linked content or advertising.

Staff must always check videos before using them and use a school-safe platform like LGfL TRUSTnet's Video Central HD (vchd.lgfl.net), which has no adverts, is designed for use with pupils, and is linked to school accounts.

Data Protection and Security

The Department for Education document KCSIE 2022 Part 2 para 119 states that the:

> *Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.*

The Headteacher, Data Protection Lead and Governors work together to ensure a GDPR compliant framework for storing data, but which ensures that child protection is always put first and data- protection processes support careful and legal sharing of information.

Staff are reminded at the annual Housekeeping INSET that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. INSET also reminds staff who the key contacts are to report any incidents where data protection may have been compromised. All staff are DBS checked and records are held in a single central record.

The use of security software to encrypt all non-internal emails is essential for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The school ensure that all staff sign its *Acceptable Use* Policy which makes clear all responsibilities and expectations with regard to data security.

The school has approved educational web filtering (see below) across our wired and wireless networks. We can monitor emails, blogs and online platforms to ensure compliance with the *Acceptable Use Policy*.

Staff have secure areas on the network to store documents and photographs.

The school asks staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which no longer need to be stored.

Management Information Systems (MIS) and Data transfer

Staff have secure areas on the network to store sensitive files. The school requires staff to log-out of the system when leaving their computer.

All servers are in lockable locations and managed by DBS checked staff;

Details of all school-owned hardware is recorded on a hardware inventory.

The school follows the Learning Authority guidelines for the transfer of data, such as MIS data or pupil reports, professionals working in the Local Authority or their partners in Children's Services, Family Services, Health, Welfare and Social Services.

The school requires personal or sensitive material to be encrypted if the material is to be removed from school and endeavours to limit such removal. We have an approved remote access solution so designated staff can access sensitive and other data from home without the need to take data home.

The school uses the *DfE S2S* site to securely transfer CTF pupil data files to the DfE or to other schools. Furthermore, we use the Pan-London Admissions system to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag for additional security.

The school stores sensitive or special category written material in lockable storage cabinets in a lockable area.

The school securely backs up the computer files of the following staff members - School Administrators, Deputy Head, Business Manager and the Headteacher – digitally on-line using LGfL's GridStore remote secure back up.

The school complies with the *Waste Electrical and Electronic Regulations* (2013) and/or the *Waste Electrical and Electronic* (amendment) Regulations (2018) for the disposal of IT equipment. For systems where any protected or restricted data has been held (servers/photocopiers) we will obtain a certificate of secure deletion. Portable equipment loaned by the school for use by staff at home, where used for any protected data is disposed of through the same procedure.

Paper based sensitive information is shredded using a cross-cut shredder.

Passwords

The school makes it clear that staff and pupils must always keep their passwords private and must not share them with others. If a password is compromised the Headteacher must be notified immediately.

All staff have their own unique username and password to access school systems and staff are responsible for keeping their passwords private.

Staff are required to compose strong passwords.

Staff are required to change their passwords for our MIS Administration program (INTEGRIS) every 90 days.

Electronic Communication

1. Email

Staff use *Staff Mail* for all school emails. The system is linked to the USO authentication system and is fully auditable, trackable and managed by *LGfL TRUSTnet* on behalf of the school. This is for the mutual protection and privacy of all staff and parents, as well as to support data protection.

Email is the chosen means of electronic communication to be used between staff and parents. Use of a different platform must be approved in advance by the Data-Protection Officer/Headteacher. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL or to the Headteacher.

School communication through email is only authorised when using the above-mentioned system. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Appropriate professional behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is, or could be, construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school into disrepute or compromise the professionalism of staff. Staff or pupil personal data should never be sent/shared/stored on email. If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL TRUSTnet.

Internally, staff should use the school network, including when working from home when secure remote access is available via the RAV3 system.

There are pupil opportunities to email within the school but not to external accounts. The service provided by *LGfL TRUSTnet* is called SafeMail and can be applied upon request via support.lgfl.net for all pupils or a particular year group.

Pupils and staff are allowed to use their email systems for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or adult sites may be blocked and not arrive at their intended destination.
Permission can be sought for the Technician to monitor a person's account if there are reasonable suspicions of inappropriate usage.

2. School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Department for Education has determined information which must be available on a school website. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to the Deputy Head.

When other staff upload information for the website, they are asked to remember that:

- Schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.

- Where pupils' work, images or videos are published on the website, their identities are protected and full names are not published; also images are not to be saved with a filename that includes a pupil's full name.

Digital Images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos beyond internal assessment and display purposes; for example, to be published on the website or in a newsletter. Parents and carers can at any time decide to withdraw their consent, but they should do so in writing.

Whenever a photo or video is taken or made, the member of staff taking it will check the latest photograph permission database before using it for any purpose.
Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's *Acceptable Use Policy*, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing or posting images, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Device Usage

1. Personal Devices and Bring Your Own Device (BYOD)

Pupils in Year 6 are allowed to bring mobile phones in for communication purposes - before and after school - they are stored away during school hours and returned when they are dismissed at the end of the school day. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions outlined in the *Behaviour for Learning Policy* and the possibility of a withdrawal of mobile phone privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought) and this should be done in the presence of a member staff.

Parents are encouraged to leave their phones in their pockets when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

During the school day; urgent messages will be passed via the school office.

Network and Internet Access on School Devices

Pupils are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use within the framework of the *Acceptable Use Policy*. All such use is monitored.

Volunteers and contractors should not have access to the school network or wireless internet on personal devices. All internet traffic is monitored.

Parents can access the guest wireless network but have no access to networked files/drives. All internet traffic is monitored.

School and Residential Trips

For school trips/events away from school, teachers will not use their personal mobile for any communications with parents, they must always contact the school. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or pupil accessing a teacher's private phone number.

Searching and Confiscation

In line with the DfE *guidance 'Searching, screening and confiscation: advice for schools'*, the Headteacher and staff have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Communication

This policy will be communicated to staff and the school community in the following ways:

- Policy to be uploaded to the school website;
- Policy to be part of the school induction pack for new/temporary staff;
- This policy forms part of the annual INSET (Housekeeping/Health and Safety/Safeguarding);
- Acceptable Use Policies discussed with staff annually;
- Acceptable Use Policies for pupils signed annually;
- Acceptable Use Policies to be issued to community on entry to school;
- E-safety rules shared with pupils and signed at the beginning of academic year;

- Updates and training for staff in line with new guidance/legislation/policy/concerns.

Inclusion/Equal Opportunities

Equal access to the curriculum is given to all staff and children regardless of ability, gender, culture or ethnic origin or other protected characteristics. Rhodes Avenue complies with its duties under the Equality Act 2010 and all staff will have due regard to the need to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the abovementioned Act. The school celebrates diversity and encourages inclusion.

Review and Monitoring

This Online Safety Policy is referenced with other school policies and documents:

- Use of Social Medeia Policy;
- Safeguarding/Child Protection and Procedures Policy;
- Anti-bullying Policy;
- Behaviour for Learning Policy;
- GDPR Policy;
- Data Protection Policy;

There is widespread ownership of this policy and it has been agreed by the Headship team and approved by the Governors. All amendments to this policy will be disseminated to all members of staff and the school community.

This policy will reviewed every two years, according to the schools policy schedule or when any significant/important technological changes or statutory guidance occurs.

Persons Responsible for the review of this policy

Headteacher
Deputy Head
Designated Safeguarding Lead
Curriculum Committee

Additional Online Safety Advice

Childnet provide guidance for schools on cyberbullying

Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

London Grid for Learning provides advice on all aspects of a school or college’s online safety arrangements

NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college’s online safety arrangements

Safer recruitment consortium “guidance for safe working practice”, which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

Online safety guidance if you own or manage an online platform DCMS advice

A business guide for protecting children on your online platform DCMS advice

UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Online safety- Remote education, virtual lessons and live streaming

Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students

Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely

London Grid for Learning guidance, including platform specific advice

National cyber security centre guidance on choosing, configuring and deploying video conferencing

UK Safer Internet Centre guidance on safe remote learning

Online Safety- Support for children

Childline for free and confidential advice

UK Safer Internet Centre to report and remove harmful online content

CEOP for advice on making a report about online abuse

Online safety- Parental support

Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online

Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

Parentzone provides help for parents and carers on how to keep their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment

#Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships

APPENDIX

Acceptable Use Policy for Staff

KS1 Acceptable Use Policy for Pupils

Lower KS2 Acceptable Use Policy for Pupils

Upper KS2 Acceptable Use Policy for Pupils

Acceptable Use Policy for Parent and Carers

Photographic and Filming Policy for Parents and Carers

Pupil Digital Media Consent Declaration Form

KS1 Internet Safety Rules

KS2 Internet Safety Rules

Online Safety Form

Acceptable Use Policy for Staff, Governors and Volunteers

I have read and understood the school's *Online Safety Policy* and agree to abide by the approaches and guidance outlined therein both for my behaviour as an adult and for enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with school policy without delay.

I understand the responsibilities listed for my role in the school's *Online Safety Policy* and agree to abide by them.

I understand my duty to support a whole-school safeguarding approach and support the principle that 'safeguarding is a jigsaw' and that my concern might 'complete the picture' if I report it. Consequently, I will report any behaviour – staff or pupils - which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (DSL) or the Headteacher

I will follow the guidance in the *Online Safety Policy* for reporting incidents but also any concerns I might think are unimportant –I have read the sections on handing incidents and concerns about a child in general, youth produced sexual imagery (sexting), bullying, sexual violence and harassment, misuse of technology and social media. I have read *Keeping Children Safe in Education* (2018).

I understand that the internet and devices used in school, school-owned devices and networks out of school may be subject to filtering and monitoring.

I have read the school's *Use of Social Media Policy.* I understand my professional responsibilities and will promote positive online safety. I will model safe, responsible and positive behaviours in my own use of technology, including 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. If I am not sure if I am allowed to do something, I will not do it.

I will not contact or attempt to contact any pupil or access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's *Online Safety Policy*. I will report any breach of this by others or attempts by pupils to do the same.

I understand the importance of upholding my online reputation, of the school and of the teaching profession and I will do nothing to impair either.

I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.
I agree to adhere to all provisions of the school *Data Protection* and *GDPR* policies at all times, (on-site or off-site or using a school or non-school device) and will ensure I do not access, nor attempt to access, store or share any data which I do not have express permission for.

I will respect copyright and intellectual property rights.

I will protect my passwords/logins and I will immediately change passwords and notify the Headteacher if I suspect a breach.

I understand that the recording, taking and sharing of images, video or audio on a mobile phone is not authorised unless it has been agreed by the Headteacher, then uploaded to the school network and deleted from the mobile device.

I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

I will use school devices and networks/internet/platforms/other technologies for school business and I will not use these to access material that is illegal or in any way inappropriate for an education setting
I will only use the school's approved staff e-mail system – London Grid for Learning – for school business including communication with parents.

I will not attempt to bypass security or monitoring, I will look after devices loaned to me, and will notify the school of "significant personal use".

I will report any accidental access to, receipt of inappropriate materials, or any filtering breach to the DSL or Headteacher.

I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

I understand and support the commitments made by pupils, parents, colleagues, governors and volunteers in their *Acceptable Use Policies* and will report any infringements in line with school procedures.

I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

____

To be completed by Governors/Staff/Volunteers

Signature: ____________________________________ Date: ____________

Name: ____________________________________

Role: ____________________________________

RHODES AVENUE
PRIMARY SCHOOL

KS1 Acceptable Use Policy for Pupils

Name: ______________________ **Class:** ______________

	TICK
I **KNOW** my trusted adults	□
I am **KIND** and polite to everyone on-line	□
I will **TELL** a trusted adult if I get upset, worried, scared or confused when I am on-line	□
I will not **SHARE** my password	□
I will **CHECK** with a trusted adult before I use new websites, games or apps	□
I will not keep **SECRETS** just because someone asks me to	□
I **STAY SAFE** because I never share private things like my name, address or telephone number	□
I **KNOW** that people online aren’t always who they say they are	□
I will not change my **CLOTHES** in front of a computer or a tablet camera	□

My trusted adults are:
School: ______________________ Home: ______________________

Signed:______________________ Date: ______________

RHODES AVENUE
PRIMARY SCHOOL

Lower KS2 Acceptable Use Policy for Pupils

I know who my trusted adults are.

I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use apps, sites and games if a trusted adult says I can.

I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.

I keep my passwords to myself and reset them if anyone finds them out.

I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.

I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

I know it's not my fault if I see or someone sends me something bad – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell someone.

I will only communicate and collaborate online – with people I know and have met in real life or that a trusted adult knows about.

I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.

I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour to a trusted adult

I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.

I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult at school.

Outside school, my trusted adults are: ______________________________

Signed: ____________________

Name: ____________________ Class: ____________________
Date: ____________________

Upper KS2 Acceptable Use Policy for Pupils

I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use apps, sites and games if a trusted adult says I can.

I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.

I keep my passwords to myself and reset them if anyone finds them out.

I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.

I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

I know it's not my fault if I see or someone sends me something bad – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell someone.

I will only communicate and collaborate online – with people I know and have met in real life or that a trusted adult knows about.

I know new friends aren't always who they say they are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. If I want to meet them, I will ask a trusted adult, and never go alone or without telling an adult.

I don't do public live streams on my own – and only go on a video chat if my trusted adult knows I am doing it and who with.

I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.

I keep my body to myself online – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult. I say no online if I need to – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.

I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.

I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see them.
I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.

I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

I use safe search tools approved by my trusted adults. I know I can’t believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult at school

Outside school, my trusted adults are: ____

Signed: ________________________

Name: ________________________ Class: _____________________________

Date: __________________________

RHODES AVENUE
PRIMARY SCHOOL

Parent and Carer Acceptable Use Policy

I understand that Rhodes Avenue Primary School uses technology as part of the daily life of the school.

I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.

I realise that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring.

I will promote positive online safety and model safe, responsible and positive behaviours in my 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.

The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous.

The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.

I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety

I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet.

I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

I can find out more about online safety at Rhodes Avenue Primary School by reading the Online Safety Policy which is available to download from the school's website and can talk
to the Headteacher or the Safeguarding Designated Leader if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I have read, understood and agreed to this policy.

Signature: ______________________

Name of parent/guardian: _________

Parent/guardian of: _______________ Date: _______________

Photographic and Filming Policy for Parents and Carers

This policy applies to sporting events, parents' evenings, plays, assemblies, school trips and any other school event or gathering, whether on school premises or beyond.

The school appreciates the importance families attach to digitally recording key or important moments in their child's development and the general rule is that parents and carers may take photos and videos of the children in their care, **for personal use only**. There may be rare exceptions to this, and we will let you know in advance of events where no filming is possible.

When you capture footage or still images of your children, there is a strong possibility that other children will also be visible or audible. For this reason, no such content should be shared publicly.

Live streaming of images, whether public or private, is not permitted and we request that you do not use any streaming platforms or 'live' features (e.g. Facebook Live) to stream events/circumstances as they occur. You may be asked to leave the premises or event if this takes place.

There are several important reasons for this:

- Some children are deemed at risk by local authority safeguarding and child protection authorities; their image must never be put online for their own protection. You are very unlikely to know who these children are. Others may have complex family backgrounds which mean that sharing their image could have unforeseen consequence. There is the real possibility you could endanger a child by sharing their image in an identifiable context (e.g. where the school is easy to identify and locate).

- Express consent is needed from parents to comply with data protection legislation, which has been been enhanced under GDPR and the new Data Protection Bill. Sharing could otherwise potentially incur fines for contravention of data protection rules.

- Some families may object for religious or cultural reasons, or simply for reasons of personal privacy.

- We encourage young people at our school to think about their online reputation and digital footprint: online photos and videos do not simply disappear when they are deleted them from accounts.

- Where possible, we will take appropriate staged group shots of pupils whose parents/carers have given appropriate photographic permissions and make these available to you. Equally, and again wherever possible, we will ensure there is time for parents to take photographs of their own children for example by approaching the stage after a performance.

RHODES AVENUE
PRIMARY SCHOOL

Pupil Digital Media Consent Declaration Form

Dear Parents/Carers,

Technology provides many perceived benefits; for example, mass communication through social networks and the sharing of digital imagery. However, it is important that educational institutions continually review and consider the impact of such developments on its community and the wellbeing concerns that some parents/carers may have with technological change.

Posting images on social media sites is instant and can be rewarding and celebratory. Additionally, images of Rhodes Avenue pupils in school publications and on the school website or videos of their performances can be motivating for the children involved, and provide a good opportunity to promote the work of our school.

Current data protection legislation and *General Data Protection Regulation* (2018) requires schools to seek parental/carer consent prior to publication of any images. Consequently, we would like to know if you give or do not give consent to images/videos of your child being used for school purposes.

If you choose not to give consent your child's name will be entered onto Rhodes Avenue's *Digital Media Register of Non-Consent* and Rhodes Avenue Primary School will take every reasonable precaution to ensure that images/videos of the child will not be published. Please be aware that many of our performances are filmed – Christmas Shows, Class Assemblies and Musical Performances - and in order comply with your declaration, that your child images are not to be used/published, the school cannot guarantee that your child will be able to take part in productions that are filmed.

Please complete and return this declaration to the school office. You may at any time change your mind about whether you wish to give or not give consent. You just need to complete a new form which can be obtained from the school office.

....

Rhodes Avenue School's Pupil Digital Media Consent Declaration Form

Child's Name: ______________________________ Current class: ______________________

Parent/Carer's Name: _________________________________

[ ] **YES** - I give my consent for images identifying my child by his/her facial features to be used in school publications or online. I can change my mind in the future if I would like to.

[ ] **NO** - I do not give my consent for images identifying my child by his/her facial features to be used in school publications or online. I can change my mind in the future if I would like to.

Signed: ________________________________ Date: _______________

KS1 Safe Internet Rules

- I will always ask permission before using the internet.
- When on-line I will not tell people my: name, phone number, address or password.
- I will tell an adult if I see anything that upsets me.
- I will remember to ‘Zip it!’ ‘Block it!’ ‘Flag it!’.

KS2 Safe Internet Rules

- I will always ask permission before using the internet.
- When on-line I will not tell people my: ○ name; ○ phone number; ○ address; ○ password.
- I will not arrange to meet someone that I have met on the internet unless a trusted adult has given permission or accompanies me.
- I will not send a photograph or video that can be used to identify myself, my family or friends unless a trusted adult has given me permission.
- Messages that I send will always be polite and sensible.
- I will not reply to unkind messages but will tell a trusted adult.
- I will tell an adult if I see anything that upsets me.
- I will not open files, emails or documents from people I do not know.
- I will remember to ‘Zip it!’ ‘Block it!’ ‘Flag it!’.

Online Safety Form			
Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review			
Signature (Head teacher)		**Date:**	
Signature (Governor)		**Date:**	