Rokeby Park Primary School

Online Safety Policy

Rokeby Park Primary School
Gershwin Avenue
Hull
HU4 7NJ
Tel: 01482 508915
Email: admin@rokeby.hull.sch.uk

Online Safety

Online Safety encompasses internet technologies and electronic communications, for example, mobile phones as well as collaboration tools and personal publishing. At Rokeby Park Primary, we endeavour to highlight the benefits and risks of using technology and teach the pupils how to safeguard themselves online.

The school's online safety policy will operate in conjunction with other school policies and procedures that should also be referred to:

- Safeguarding
- Whistleblowing
- Positive Behaviour Policy
- Guidance on Safer Working Practice
- Staff Code of Conduct
- Data Protection
- Curriculum

The following local/national guidance should also be read in conjunction with this policy:

- Hull Local Safeguarding Children Partnership, Guidelines and Procedures (2019)
- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2020
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

At Rokeby Park Primary School, the Online Safety Lead who is also the Deputy Designated Safeguarding Lead (Amy Gawthorpe) works in close conjunction with the Designated Safeguarding Lead (Sally Chaytor) and Computing Lead (Rosie Driscoll) in school.

For clarity, the online safety policy uses the following terms unless otherwise stated:

Users – refers to all staff, pupils, governors, volunteers and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school, e.g. parent, guardian, carer.

School – any Rokeby Park Primary School business or activity conducted on or off the site, e.g. visits, conferences, trips etc.

Safeguarding is a serious matter. At Rokeby Park Primary, we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as online

safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.
The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to the student or liability to the school

This policy is available for anybody to read on our school website. All members of staff will read and sign the Staff Acceptable Use Policy. A copy of the students' Acceptable Use Policy will be sent home with students at the beginning of each academic year. Upon return of the signed copy of the Acceptable Use, pupils will be permitted access to Rokeby Park Primary School's technology including the Internet.

Learning and Teaching

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Rokeby Park Primary School will have an annual training programme which is suitable to the audience.

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

• We will provide a curriculum/Jigsaw curriculum/Computing curriculum and other lessons which have online safety lessons embedded throughout.

• We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.

• We will discuss, remind or raise relevant online safety messages with pupils routinely, wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital material.

• Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum area.

• Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.

• We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.

• When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.

• Pupils will be taught about the impact of online bullying and know how to seek help

if they are affected by any form of online bullying (see Anti-Bullying Policy).

• Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Remote Learning

• We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and through Microsoft Teams.

• We expect pupils to follow the same principles, as outlined in the school's Acceptable Use policy, whilst learning at home.

• If our school chooses to communicate with pupils via Teams etc. pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.

• Any significant behavioural issues occurring on any virtual platform must be recorded, reported on CPOMs and appropriate sanction imposed. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.

• Staff should be mindful that when dealing with any behavioural incidents which occur online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

Staff Training

Staff at Rokeby Park Primary School receive regular information and training on online safety issues, as well as updates as and when new issues arise.

• As part of the induction process all staff receive information and guidance on the Online Safety Policy, the school's Acceptable Use Policy and Safeguarding Policy.

• All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

• All staff will be encouraged to incorporate online safety activities and awareness within their curriculum areas.

Roles and Responsibilities

Governing Body
The Governing Body is accountable for ensuring that Rokeby Park Primary School has effective policies and procedures in place.

Headteacher
Reporting to the Governing Body, the Headteacher has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Lead, as indicated below.

The Headteacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.

- The designated Online Safety Lead has had appropriate training in order to undertake the day to day duties.

- All Online Safety incidents are dealt with promptly and appropriately.

Online Safety Lead
The day-to-day duty of Online Safety Lead is devolved to **Mrs Amy Gawthorpe.**
The Online Safety Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Headteacher.

- Advise the Headteacher and governing body on all online safety matters.

- Engage with parents and the school community on online safety matters at school and/or at home.

- Liaise with the local authority, IT technical support and other agencies as required

- Retain responsibility for the online safety log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical online safety measures in the school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or Technical Support.

- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

Technical Support Staff

At Rokeby Park Primary School, we have a Smoothwall filtering system in place which is managed by the school and RM. Banned phrases and websites are identified which ensures that pupils can only access appropriate websites and materials on our school devices. RM staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit for purpose, up to date and applied to all capable devices.

- Windows (or any other operating system) updates are regularly monitored and devices updated as appropriate.

- Any online safety technical solutions such as internet filtering are operating correctly.

- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Lead immediately.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety Lead and Headteacher.

- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).

- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

We also use a service called ESafe to help protect pupils and staff members from safeguarding risks and detect any early signs of safeguarding concerns. The service monitors all activities on IT devices through a triple-lock protection system. They look at trends and emerging trends through words and phrases as well as images searched for on devices. Trained analysts monitor usage and activity to determine the severity and risks associated and grade the threat levels. ESafe provide the school with data so that they can intervene and act appropriately.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher or the Online Safety Lead.

- Any online safety incident is reported to the Online Safety Lead (and incidents are recorded on CPOMs), or in their absence to the Headteacher. If you are unsure, the matter is to be raised with the Online Safety Lead or the Headteacher to make a decision.

All Pupils

The boundaries of use of equipment and services are given in the Student Pupil Acceptable Use Policy; any deviation or misuse of equipment or services will be dealt with in accordance with the Positive Behaviour Policy.

- Online safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.

- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Parents and Carers

Parents play the most important role in the development of their children; as such Rokeby Park Primary School will ensure that opportunities are made to support parents so that they have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, social media, Ping bulletin advice, the school website and other events in school, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand that Rokeby Park Primary School needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the Pupil Acceptable Use Policy before any access can be granted to school equipment or services.

Technology

Rokeby Park Primary School uses a range of devices including PCs, laptops and iPads. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – We use Smoothwall software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites (appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner). The Computing Lead, Online Safety Lead, RM and ESafe are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – We use a system that prevents any infected email to be sent from school, or to be used by school. Infected is defined as: an email that contains a virus or script that could be damaging or destructive to data; spam email such as a phishing message.

Encryption - Any personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Any personal data that leaves the school site will only do so on an encrypted device. Any breach (i.e. loss /theft of device such as laptop or Ipad) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Chief Operating Officer of The Constellation Trust to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – All staff and pupils will be unable to access any device without a unique username (passwords for staff). Staff passwords will be changed if there has been a compromise.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated daily for new virus definitions. I.T Support will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns.

Mobile phones- No pupil should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be locked away until the end of the day. Mobile phones and personally-owned devices that belong to members of staff or visitors in the school will be not be taken into any areas where children will be during school hours, and

will be kept in lockers or locked away. The Safeguarding Lead, Deputy Safeguarding Lead and the Headteacher will have a mobile phone on them (school mobile in the classroom) to enable them to access CPOMs. The Site Facilities Lead will be contacted through a walkie talkie or a school mobile phone during school hours.

Safe Use

Internet – Use of the internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the Staff Acceptable Use Policy and to pupils upon signing and returning their acceptance of the Pupil Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work based emails only. Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted. The secure email system (EDT) should be used at all times to send sensitive data outside the school system.

Photos and Videos – Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Social Networking – There are many social networking services available. Rokeby Park Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within the school and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Lead who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Facebook – used by the staff in school as a broadcast service
- Twitter – used by the school as a broadcast service

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be ‘followed’ or ‘friended’ on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission for photographs and videos to be used on social media, websites and around school will be sought from parents when children join our school, and updated if anything changes. This information will be collected and all members of staff will be made aware of who and who cannot be photographed/ videoed.
- There is to be no identification of any pupil using first name and surname; first name only is to be used.
- Where services are ‘comment enabled’, comments are to be set to ‘moderated’.
- All posted data must conform to copyright law; videos and other resources that are not originated by Rokeby Park Primary School are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use.

Staff will not post inappropriate content or participate in any conversations which will be damaging or be deemed detrimental to the image of the school. Members of staff who hold

a personal account should not have pupils (past or present) as their 'friends' or 'followers' on social media. Staff should also not have any parents or as their 'friends'/ 'followers', unless the 'relationship' with the parent pre-exists before child starts school. Please see guidance for professionals working with young people document.

Dojo- ClassDojo is a school communication platform that teachers and families use every day to develop parental partnerships between school and home and it is also used as part of our Positive Behaviour Policy. Teachers and parents can send messages to each other via ClassDojo regarding pupils, what they have been learning in the classroom and any achievements. In the event of remote learning taking place, parents are encouraged to send in photographs of their child's work so that teachers can support and celebrate achievements. Communication with parents should only take place on ClassDojo during the hours of 8am - 6pm and conversations should be professional.

Notice and take down policy – should it come to the attention of Rokeby Park Primary School that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents – Any online safety incident should be brought to the immediate attention of the Online Safety Lead, or in their absence the Headteacher. The Online Safety Lead will assist in taking the appropriate action to deal with the incident. Incidents will be documented on CPOMs and actions will be taken by appropriate members of staff. An important element of online safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report online safety incidents promptly so that they may be dealt with effectively. The school has incident reporting procedures in place and records incidents on the secure electronic reporting system called CPOMs. All staff have restricted access to the system with the ability to report any online/safeguarding issue at any time. Key members of staff hold full access keys which gives them the ability to respond to, action and analyse incidents.

Online sexual harassment- Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats). Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our school follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Radicalisation Procedures and Monitoring- It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via Safeguarding Lead). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils.

CCTV- The school uses CCTV in some areas of school property as a security measure. CCTV may be used by the Headteacher, SLT or site facilities officer to look at incidents for behaviour, safety and for safeguarding purposes. Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

Screening, Searching and Confiscation- The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm;
- disrupt teaching;
- break school rules;
- commit an offence;
- cause personal injury;
- damage property.

General Data Protection (GDPR) and online safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the Trust's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

Reviewed: by C Smith & A Gawthorpe