Rokeby Park Primary School

Online Safety Policy

Reviewed: March 2018
Next review: March 2019

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

E-Safety

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-Safety Policy will operate in conjunction with other policies including those for ICT, Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Safeguarding.

At Rokeby Park Primary School, the ICT Coordinator will be the e-Safety Coordinator and will work in conjunction with the Child Protection Co-ordinator.

For clarity, the e-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 School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-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 e-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 the school website; upon review all members of staff will sign as read and understood both the e-Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students' Acceptable Use Policy will be sent home with students at the beginning of each academic year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to Rokeby Park Primary School's technology including the Internet.

Roles and Responsibilities

Governing Body

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

- Review this policy at least annually and in response to any e-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-Safety incidents were appropriately dealt with and ensure the policy in managing those incidents

- Appoint one governor to have overall responsibility for the governance of e-Safety at the school who will keep up to date with emerging risks and threats through technology use and receive regular updates from the Headteacher in regards to training, identified risks and any other incidents

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

The Headteacher will ensure that:
- E-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 e-Safety Officer has had appropriate training in order to undertake the day to day duties
- All e-Safety incidents are dealt with promptly and appropriately

E-Safety Officer
The day-to-day duty of e-Safety Officer is devolved to **Mrs Amy Gawthorpe.**
The e-Safety Officer 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, governing body on all e-Safety matters
- Engage with parents and the school community on e-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 e-Safety log ; ensure staff know what to report and ensure the appropriate audit trail
- Ensure any technical e-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 ICT Technical Support
- Make themselves aware of any reporting function with technical e-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

ICT Technical Support Staff
Technical support 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 e-Safety technical solutions such as Internet filtering are operating correctly
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-Safety officer and Headteacher
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

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
- Any e-Safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in their absence to the Headteacher. If you are unsure, the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision
- The reporting flowcharts in this e-Safety Policy are understood

All Pupils
The boundaries of use of ICT equipment and services are given in the pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy

E-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.

Parents and Carers
Parents play the most important role in the development of their children; as such Rokeby Park Primary School will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, the school website and other events the school will keep parents up to date with new and emerging e-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 student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Rokeby Park Primary School uses a range of devices including PCs, laptops, netbooks, Huddles 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 ICT Coordinator, e-Safety Officer and ICT Support 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 USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

eSafe: We use a service called eSafe to help protect pupils and staff members from safeguarding risks and detect the 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.

Hudls- All Hudls must have kids place active at all times and pupils to only be given access to the apps they need.

Passwords – All staff and pupils will be unable to access any device without a unique username (passwords for staff). Staff passwords will change 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. ICT 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 pupils 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 (3:30pm). 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 Officer, Deputy safeguarding officer and the Headteacher will have a mobile phone on the (school mobile in the classroom) to enable them to access CPOMs. The Site Facilities Officer will be contacted through a walkie talkie during school hours and before/ after school he will be contacted by contractors through a mobile phone.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-Safety Policy and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the 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. 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 e-Safety Officer 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 slips (via the school Photographic Policy) must be consulted before any image or video of a child is uploaded
- There is to be no identification of 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 to 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.

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 e-Safety incident is to be brought to the immediate attention of the e-Safety Officer, or in their absence the Headteacher. The e-Safety officer will assist you in taking the appropriate action to deal with the incident and to fill out the incident log. 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 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 academy follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Training and Curriculum – 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.

E-Safety for pupils is embedded into the curriculum; whenever computing is used at Rokeby Park Primary School, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupils' learning.

E-Safety is embedded through the all areas of the curriculum, particularly computing and PSHCE; assemblies and participation in national e-Safety week.

As well as the programme of training, we will establish further training or lessons as necessary in response to incidents.

Review
This policy will be reviewed annually.
Reviewed: March 2018 by C Smith, A Gawthorpe & S Kelsey
Next review date: March 2019

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign the Acceptable Use Policy Sheet.

Internet Access – You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-Safety incident, reported to the e-Safety Officer and an incident sheet should be completed on CPOMs.

Use of computer- You must not let children or other members of staff use the computer when you are logged on due to members of staff having different accesses, for example, safeguarding. All browsing will be monitored to ensure safe use.

Social Networking- is allowed in school in accordance with the e-Safety Policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become 'friends' with parents or pupils on personal social networks (past or present).

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords – Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff, student or ICT Support.

Data Protection – On no occasion should data concerning personal information be taken offsite.

Share Point- Any data or information that can be linked to a child or the school should be saved onto Share Point to be accessed by staff and others. Information should not be saved onto any portable device, for example, laptops or memory sticks (including encrypted memory sticks).

Personal Use of School ICT – You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos – You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings). Staff must ensure that they know which children can be / cannot be photographed when uploading any image/ video (see up to date permissions).

Use of Personal ICT – Use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by ICT Support and the e-Safety Officer. All personal ICT equipment must be PAT Tested.

Viruses and other Malware – any virus outbreaks are to be reported to the e-Safety Officer/ICT Support as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like Health and Safety, e-Safety is the responsibility of everyone to everyone. As such you will promote positive e-Safety messages in all use of ICT whether you are with other members of staff or with students.

Devices- Any member of staff taking school devices home (Ipad) must make sure that they are not used by anyone else, they are used only for work purposes and that they are password protected. Devices must be kept secure and should not be left in cars or insecure locations.

Acceptable Use Policy Sheet– Staff

I confirm that I have received a copy of Rokeby Park Primary School's e-Safety Policy and Acceptable Use Policy. I confirm that I have read and understood both policies.

Name:

Signature: Date:

Name:

Signature: Date:

Name:

Signature: Date:

Name:

Signature: Date:

Name:

Signature: Date:

Name:

Signature: Date:

Name:

Signature: Date:

Name:

Signature: Date:

Acceptable Use Policy – Pupils

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for school work that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment; if I accidentally damage something I will tell my teacher.

I will not - use other people's usernames/ log on.

I will not - share personal information online with anyone.

I will not - download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (Pupil):

Date: