ROOKERY SCHOOL E-SAFETY POLICY

Our e-safety policy has been written by the school, based on guidance from LGfL. It has been agreed by the senior leadership team and approved by governors following discussions with parents and pupils. It will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

The e-safety policy is referenced from within other school policies: safeguarding policy and Promoting positive behaviour policy.

Date	02/02/2017
Author	Laura Neal (E-safety co-ordinator)
Approved by head teacher	
Approved by Governing Body	
To be Reviewed	

Contents

1. Introduction and Overview

School Statement

We believe that education lies at the heart of E-safety in our school. If our children are well informed and aware of E-safety issues, then we can support them in taking the steps necessary to keep safe online, now and in the future.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Rookery School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Rookery School.
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- 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.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse
- exposure to terrorist and extremist material and radicalisation
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))

- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ofsted, Inspecting safeguarding in schools, 2014)

Scope (adapted from SWGfL)

This policy applies to all members of Rookery's community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Rookery School.

Responsibilities

Role	Key Responsibilities
Headteachers	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident.
E-Safety Co-ordinator	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • to ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • to ensure that an e-safety incident log is kept up to date • facilitates training and advice for all staff • liaises with relevant agencies
Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities

Role	Key Responsibilities
Network Manager/technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that the use of the *network / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures • To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator using e-safety incident report • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
	• to understand the importance of misuse or access to inappropriate materials and are aware of the consequences • to realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to consult with the school if they have any concerns about their children's use of technology

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school can not accept liability for material accessed, or any consequences of Internet access.
- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Promoting Positive Behaviour for Learning Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Teaches using the ‘Switched On Computing’ curriculum. This scheme integrates the teaching of E-safety into each of the computing units throughout the year.
- The scheme covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will ‘groom’ young people
    - To understand the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to seek 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 CLICK CEOP button.

- The schools PSHE and SMSC (spiritual, moral, social and cultural) scheme, ‘Jigsaw’, also educates children on a range of E-safety issues including cyber and homophobic bully and internet safety.
- Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Displays in the community and ICT rooms with E-safety advice for parents
    - Parents presentations on safe Internet use at home
    - Information leaflets; in school newsletters; on the school web site;
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear

3. Expected Conduct and Incident management

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and reported to the school's senior leaders.
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example admin@rookeryschool.co.uk for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Learning platform

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools LEARNING PLATFORM will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform;

Social networking

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority

- **Internet access, security (virus protection) and filtering**

This school:

- Has filtered secure broadband connectivity
- Uses Smoothwall filtering system which blocks sites that fall into categories such as pornography, gaming, sites of an illegal nature, race hatred,
- Filtering is in place to ensure the school protects children from terrorist and extremist material, complying with the Prevent Duty.
- Ensures network is healthy through use of antivirus software etc. and network set-up so staff and pupils cannot download and execute files;
- Uses DfE approved systems such as Smoothwall, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;
- Uses security time-outs on Internet access where practicable / useful;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment or secure platforms;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;

    - Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
    - Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  This school
    - Uses individual, audited log-ins for all staff;
    - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
    - Has additional local network auditing software installed;
    - Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- All pupils have their own unique username and password which gives them access to the Learning Platform
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off or lock a computer when they have finished working or are leaving the computer unattended;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 4.00pm to save energy;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use".

- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within an approved secure system;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Technical Solutions

- Staff have a shared area on the network to store sensitive documents or photographs.
- We use two-factor authentication for remote access into our systems.
- All servers are in lockable locations and managed by DBS-checked staff.

5. Data security: Management Information System access and Data transfer

- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Staff will sign a declaration for protection of sensitive and confidential digital data which explains the acceptable usage and storage of sensitive and confidential digital data.
- Emails sent to external agencies which contain sensitive and confidential data must be encrypted as explained in the 'sending encrypted emails document' (See appendix 7)

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated in the setting. The areas which should be considered most vulnerable include: toilets, bathrooms and changing areas.
- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide their own mobile number (by inputting 141) for confidentiality purposes.

Students' use of personal devices

- Student mobile phones should not be brought into school.
- The School accepts that occasionally there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, prior consent must be granted from the headteacher.
- Mobile phones must be handed in to the office on arrival. They will be stored in a safe in the main office and returned at the end of the school day.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school application form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-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 as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. 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 identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Adapted from: LGfL E-Safety Policy Revision 2015 v1 03/01/2015

Appendices included:

1. **Rookery E-safety Agreement Form: Parents**
2. **All staff acceptable use agreement.**
3. **KS1 acceptable use agreement**
4. **KS2 acceptable use agreement**
5. **Rookery E-safety Incident Report Form**
6. **Declaration for the protection of sensitive and confidential digital data**
7. **Sending encrypted emails**