Rushey Mead
Primary School

E-safety Policy

Policy Date:	20th September, 2021		**Version:** 1.1		
Policy Review Date:	September 2022		Headteacher Debra Bailey	Signed	Insert Date 20/09/21
Ratified by Governing Body:					
Sue Welford (Chair of Governors)			Insert Signature	Insert Date 20/09/21	

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

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

● set out the key principles expected of all members of the school community at Rushey Mead Primary with respect to the use of ICT-based technologies.

● safeguard and protect the children and staff of Rushey Mead Primary 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), substance abuse.

● lifestyle websites, for example pro-anorexia/self-harm/suicide sites

● hate sites, incitement to extremism.

● content validation: how to check authenticity and accuracy of online content and evaluate what we see online.

● How to recognise which techniques can be used for persuasion.

● Learn how to make judgements and not make assumptions.

Contact

● grooming

● cyber-bullying in all forms

● identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

● learn that people behave different online. This can include anonymity and invisibility.

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)

(Ref Ofsted inspection guidance Jan 2014)

(Ref Teaching Online safety in school – Ofsted June 2019)

Scope

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher / Designated Child Protection Lead	● 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. ● To receive regular monitoring reports from the E-Safety Co-ordinator ● To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager) ● To communicate regularly with SLT and the Safeguarding Governor / committee to discuss current issues, review incident logs and filtering / change control logs ● To ensure that an e-safety incident log is kept up to date ● Liaises with the Local Authority and relevant agencies ● Takes day to day responsibility for e-safety issues

E-Safety Co-ordinator / ICT Lead Teacher	● 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 ● Liaises with school ICT technical staff ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident ● Facilitates training and advice for all staff ● Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media ● Oversees the delivery of the e-safety element of the Computing curriculum ● Supports with remote learning, including preparing the children for how to learn remotely and ensuring that staff adopt a duty of care relating to e-safety.
Governors	● 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 and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities
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, in which passwords are regularly changed ● 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 / encryption exist to protect personal and sensitive information held on school-owned devices • **T**he school's policy on web filtering is applied and updated on a regular basis • The LA/ web filtering provider is informed of issues relating to the filtering applied • That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

	• That the use of the network, remote access, data systems and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator /Headteacher for investigation, action or 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
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 and creative commons licences.
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 Head Teacher ● 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.
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 access the school websites in accordance with the relevant school Acceptable Use Agreement. ● to consult with the school if they have any concerns about their children's use of technology
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and stored on the shared network drive
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - informing parents or carers;
    - removal of Internet or computer access for a period
    - referral to LA / Police.

- 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 Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring
The e-safety policy will be referenced from within other school policies: Child Protection policy, Anti-Bullying policy and Behaviour policy.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed regularly or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign and will be displayed throughout the school and a reminder will be displayed when a pupil logs on to the school network.
- 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;
- Has a whole school approach that embeds teaching about online safety and harm. In practice, this is about creating a culture that incorporates the principles of online safety across all elements of school life, and proactively engages staff, pupils and parents/carers. Rushey Mead Primary School promotes the agreed principles of online safety, and reviews, maintains and embeds online safety principles, as well as to model the online safety principles consistently.

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.
- Provides , as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information in school newsletters; on the school web site;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should 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
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and using images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- should have a good understanding of research skills and acting responsibly and safely online.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety Acceptable Use Agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- We refer to the *What do we do if..? Guidance document* to inform reporting pathways and appropriate responses to common e-safety issues.
- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply 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. the local authority and regional broadband grid, 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 audited and reported to the school's senior leaders, Governors /the LA.

- 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

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

This school:

- Has the educational filtered secure broadband connectivity;
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software;
- Uses DfE approved methods 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;
- Only unblocks other external social networking sites for specific purposes;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- 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 appropriate environment
- 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 e-safety co-ordinator.
- 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 users;
  - Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).
  - Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff and pupils read, accept and sign the Acceptable User Policy.
- **Photographs and videos of children**

    - To comply with the Data Protection Act 1998, we ask for parents' permission before we photograph or make recordings of pupils.
    - We follow the following rules for any external use of digital images:
        - **If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.**
    - Where showcasing examples of pupils work we **only** use their **first names**, rather than their full names.
    - If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
    - Only images of pupils in suitable dress are used.

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

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

    - staff,
    - governors,
    - pupils
    - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use VPN solution with its 2-factor authentication for remote access into our systems.

- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.
- Paper based sensitive information is shredded, using cross cut shredder

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils are not permitted to bring mobile phones into school.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

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 agreement 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;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- 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 taught that they should not post images or videos of others without their permission.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.