



Radipole Primary School

**e-Safety Policy
(including mobile technology)**

Signed:
Chair of Governors

Date of Approval: September 2017

Date of Next Review: September 2019

This policy has been reviewed in line with the 9 principles set out in the Single Equality Policy and an initial screening Equality Impact Assessment has been carried out.

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 Radipole Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Radipole 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
- 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)

Scope

This policy applies to all members of Radipole 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 Radipole 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. 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 / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"> • To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • 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	<ul style="list-style-type: none"> • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies • 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 • ensures 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 • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> • 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
Governors / E-safety governor	<ul style="list-style-type: none"> • To ensure that the school follows all current e-safety advice to keep the children and staff safe
Technology curriculum team	<ul style="list-style-type: none"> • To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly

Role	Key Responsibilities
Network technician	<ul style="list-style-type: none"> • 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 • the school's policy on web filtering is applied and updated on a regular basis • that he 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 • 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	<ul style="list-style-type: none"> • To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • To read, understand and help promote the school's e-safety policies and guidance • 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 • 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
Pupils	<ul style="list-style-type: none"> • 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
Parents/carers	<ul style="list-style-type: none"> • to support the school in promoting e-safety and endorse the Acceptable Use of Mobile Phones, where appropriate. • to consult with the school if they have any concerns about their children's use of technology

Communication:

The policy will be communicated to staff/parents/carers/community in the following ways:

- Policy to be posted on the school website / staffroom/ classrooms
- Policy to be part of school induction pack for new staff

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.
- 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 school has an e-safety coordinator who will be responsible for document ownership, review and updates.

- The e-safety policy will be reviewed bi-annually 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.

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum
 - to have annual input from Safer Schools and Community Team
 - to know how to narrow down or refine a search;
 - 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 for sexual reasons;
 - To understand the impact of cyberbullying, sexting and trolling 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.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

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:
 - demonstrations, practical sessions held at school;
 - suggestions for safe Internet use at home;

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- 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 / use of images and on cyber-bullying

Incident Management

In this school:

- 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, SSCT, 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.
- 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 through the SWGfL;
 - Uses DfE, LA or SWGfL approved systems secured email to send personal data over the Internet and uses encrypted devices or secure remote access where 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;
 - Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
 - Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
 - 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;
 - Requires staff to preview websites before use [where not previously viewed or cached] as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. [yahoo for kids](#) or [ask for kids](#) , Google Safe Search ,
 - Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
 - Informs all users that Internet use is monitored;
 - 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.
- **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.
 - 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 when they have finished working or are leaving the computer unattended;
 - Has blocked access to music/media download or shopping sites – except those approved for educational purposes;

- Makes clear that staff are responsible for ensuring that any tablet or laptop loaned to them by the school, is used to support their professional responsibilities
- 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 / LA electrical engineers
- 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;
- 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 the approved secure system in our LA
- 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;
- Reviews the school ICT systems regularly with regard to health and safety and security.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- 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;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published;
- 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;
- We do not use embedded geodata in respect of stored images

- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the Social Networking policy.

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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

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).
- 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 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.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils in year 5 and 6 may bring mobile phones into school. They must be turned off on arrival at school and handed into their class teacher. Parents and pupils are asked to sign the Acceptable Use of Mobile Phone Agreement.
- All visitors are requested not to use their phones.
- 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.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- 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.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Staff use of personal devices

- 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.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

- 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.
- If a member of staff breaches the school policy then disciplinary action may be taken.

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;
- 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
- 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.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware 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.