RAMSEY MANOR LOWER SCHOOL
E-SAFEGUARDING POLICY

Ramsey Manor Lower School is a Values Education School where our Values underpin everything we do.
We are committed to safeguarding children and providing a safe and healthy environment for all to learn and grow.

DATE ADOPTED: March 2009

Policy agreed by staff: RS   date: January 2019

Policy agreed by Governors: JB   date: January 2019

Date of next review : January 2020

Rational and Aims

E-safeguarding encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. The school's E-safeguarding policy will operate in conjunction with other policies.

E-safeguarding depends on effective practice at a number of levels:

- responsible IT use by all staff and students; encouraged by education and made explicit through published policies.
- sound implementation of E-safeguarding policy in both administration and curriculum, including secure school network design and use.
- safe and secure broadband including the effective management of filtering.
- the designated Child Protection/Safeguarding Leader (DSL) is responsible for E-safeguarding and will ensure the implementation and monitoring of this policy.

The purpose of this policy is to:

• establish the ground rules we have in Ramsey Manor Lower School for using the internet and electronic communications such as mobile phones, ipads, collaboration tools and personal publishing. It highlights the need to educate all stakeholders about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
• describe how these fit into the wider context of our discipline and PSHE policies.
• demonstrate the methods used to protect children from sites containing inappropriate material including pornography, racist or politically extreme views and violence.

Teaching and learning

• the Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
• Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
• the school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
• pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
• pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation as appropriate to their age.
• staff ensure that the use of Internet derived materials by themselves and pupils complies with copyright law.
• pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy as appropriate to their age.
• pupils are encouraged to talk about how they use IT equipment at home.

Managing the IT infrastructure

• school IT systems capacity and security is reviewed regularly.
• virus protection is updated regularly.

E-mail

• the pupils are taught to use e-mail accounts.
• the pupils are taught to immediately tell a teacher if they receive offensive e-mail.
•the pupils are taught to not reveal personal details of themselves or others in any communication, or arrange to meet anyone.
• e-mail sent to an external organisation by a pupil must be authorised before sending.

School Website & Ramsey Manor App

• the contact details on the website is the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
• the Headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.
• photographs that include pupils do not have names associated with them.
• pupils' full names are not used anywhere on the web site.
• written permission from parents or carers must be obtained before photographs of pupils are published on the school website.
• pupil's work will only be published with the permission of the pupil and parents.

The Pod

• used to inform parents of upcoming events
• promote school ethos
• regularly updated with images of our children involved with activities

Social networking and personal publishing

• social networking is only used by teachers to keep parents informed (it is no longer blocked)
• pupils are told never to give out personal details of any kind which may identify them
• pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

• if staff or pupils discover an unsuitable site, it must be reported immediately to the Designated Child Protection/Safeguard Leader.
• senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.

Managing emerging technologies

• emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
• mobile phones for pupils are not permitted in school.
• staff use of mobile phones for personal reasons is restricted to non-teaching times and must be kept in a secure place in the school. A mobile phone may be used at the discretion of the Headteacher for example during off site trips and during Forest School activities

Protecting personal data

• personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998. However the General Data Protection Regulation (GDPR) came into effect on the 25th May,2018 and we ensure compliance with GDPR (see GDPR Policy)

4. Policy decisions

Authorising Internet access

• all staff read and sign the 'Acceptable IT Use Agreement' before using any school IT resource.
• the school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access is withdrawn.
• at Key Stage 1and Reception, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
• at Key Stage 2, access to the internet will be by supervised access to specific, approved on-line materials.
• parents are asked to sign and return a consent form.

Assessing risks

• the school takes all reasonable precautions to ensure that users access only appropriate material by using the LA filtering system provided by talkstraight.

• the school audits IT provision on a regular basis to establish if the E-safeguarding policy is adequate and that its implementation is effective.

Handling E-safeguarding complaints

• complaints about internet misuse are dealt with by a member of the Senior Leadership Team.
• any complaint about staff misuse is referred to the Headteacher.
• complaints of a child protection nature are dealt with in accordance with the school's child protection procedures.
• pupils and parents are informed of the complaints procedure.

5. Communications

Introducing the E-safeguarding Policy to pupils
• E-safeguarding lessons are delivered to all pupils each term
• E-safeguarding rules are posted in all networked rooms and discussed with the pupils at the start of each year.
• pupils are informed that network and internet use will be monitored.
• Key Stage 2 pupils and their parents are informed of the child exploitation and online protection centre: thinkuknow.co.uk

Staff and the E-safeguarding Policy

• all staff have access to the school's E-safeguarding Policy and know its importance.
• staff are aware that internet traffic can be monitored and traced to the individual user.

Staff Training

Members of staff undergo E-safeguarding training.

Enlisting parents' support

• parents' attention is drawn to the school's E-safeguarding Policy in newsletters and on the school website.
• E-safeguarding training sessions are held for parents

6. <u>LINKS TO OTHER POLICIES AND DOCUMENTS</u>

Computer Security Policy
Child Protection Policy
PSHCE Policy
Anti-bullying Policy
ICT Teaching and Learning Policy
Freedom of Information Policy
Disaster Recovery Plan
Curriculum subject policies
SEND Policy
GDPR Policy

Appendix A

KS2 Pupils' Rules for Responsible Internet Use

The school has installed computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

• I will only access the system with my login and password

• I will not access other people's files

• I will only use the computers for school work and homework

• I will not bring any portable data storage into school unless specifically approved by a member of staff

• I will ask permission from a member of staff before using the internet

• I will not knowlingly download program files from the internet

• I will only e-mail or message people my teacher has approved

• Any messages I send or comments I make will be polite and sensible

• I will not give my home address or telephone number, or arrange to meet someone

• To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like

• I understand that the school may check my computer files and may monitor the internet sites I visit

Appendix B

<p align="center">**Ramsey Manor Lower School Staff, Governor and Visitor**
IT Acceptable Use Agreement / Code of Conduct</p>

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the designated safeguarding lead (DSL) .

- I will only use the school's email / internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on Target Tracker) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. (see GDPR Policy)
- I will not install any hardware or software without permission of the Computing Subject Leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safeguarding Policy and help pupils to be safe and responsible in their use of IT and related technologies.

User Signature
I consent to images of myself being taken, stored and used for professional purposes in line with school policy.
I agree to follow this code of conduct and to support the safe use of IT throughout the school

Signature …….………………….………… Date ……………………

Full Name ……………………………….......................................(printed)

Job title . . . .

These rules help us to stay
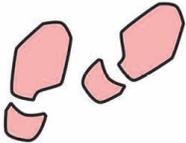safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.