Ramillies Hall School & Nursery

E – Safety Policy and Procedures

This policy is applicable to all staff (teaching and non-teaching), parents and pupils in the school and nursery. This policy should be read in conjunction with the School's Safeguarding and Child Protection Policy and Procedures. The school has a robust filtering and monitoring system.

1. OUR COMMITMENT

At Ramillies Hall School and Nursery, we are committed to safeguarding and promoting the welfare of all children, in line with the duty placed on us by Section 157/175 of the Education Act, 2002. We expect and require all staff and volunteers to share this commitment. We strongly believe that all children have the right to feel safe and to be protected from physical, sexual or emotional abuse and neglect.

2. INTRODUCTION

Digital technology has become an important part of our everyday lives both in work and personal environments, it offers exciting opportunities. The school/nursery has a duty to provide pupils with quality internet access as part of their learning experience. However, we have a responsibility under the Children Act 2004 to safeguard and promote the welfare of children.

The strategies outlined in this policy enable the staff at Ramillies to create a safe e-learning environment that:

- Promotes the teaching of E-Safety across the curriculum not solely in computing lessons;
- Protects children from harm;
- Safeguards staff in their contact of pupils and their own use of the internet;
- Ensures the school fulfils its duty of care to both staff and pupils;
- Provides clear expectations for all on acceptable use of the internet.

A broad definition of E-Safety:

All fixed and mobile technologies that children and young people may encounter, now and in the future, which allows them access to content and communications that could raise issues or pose risks to their wellbeing and safety. As a professional educational institution we will:

- Promote E-Safety across the curriculum from Nursery onwards
- Provide staff with up to date training
- Support the parents/guardians of our pupils
- Provide E-Safety resources for staff
- Ensure that schemes of work where ICT is used reflect this policy

Why internet use is important

The internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide pupils 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.

Internet use will enhance learning

Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.
Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content and make decisions affecting their privacy

The school/nursery will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
Pupils will be taught about privacy issues such as identity theft, fraud, and phishing. They will receive guidance about when to give out personal information (e.g. buying goods from secure websites) and precautions when creating 'posts' on public domains and social network areas.
Pupils will be taught how to report unpleasant internet content

Managing internet access

Information system security

- The security and robustness of school-based systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Decisions surrounding security and strategies will be made by IT support, with input from the Designated Safeguarding Leads and Officers.

Email and messaging

Email / messaging are powerful and useful tools that have become an integral part of most young people's lives. They are not intrinsically harmful and can reduce isolation and encourage collaborative learning. However, we realise that systems can be used to bully and manipulate pupils and the following principles are at the core of the policy:

- When using the school system, pupils may only use approved email accounts.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- As part of an acceptable use agreement, pupils will undertake to never send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students will be reminded that the sending of abusive messages is illegal under the Malicious Communications Act 1998.

Published content and the school website

- The contact details on the website should be the school/nursery address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher, with support from the ICT administrator, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work on the web
Open / public sites

The school understands that public sites can be used to gather information and the locations of pupils. Written permission to use photographs and work on websites will have been obtained as part of the contract signed by parents. However, unless there is need to identify a pupil (e.g. to celebrate a prize) the following guidelines should be observed:

- Pupils' full names will not normally be used on the website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully. Care will be taken when taking digital/video images that pupils are appropriately dressed.
- Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

- The school will block/filter access to social network and chat sites, depending on the way in which they are used and the characteristics they have.
- Pupils will be advised that social networking has potential dangers. As part of their responsible use agreement, they will be told never to give out personal details of any kind which may identify them or their location regardless of whether they are accessing the site from a school system or otherwise.
- Staff should use discretion when using social networking sites. They should ensure that their professionalism is maintained by refraining from "friending" past or present pupils even on a social level.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the ICT Administrator (Robert Poole).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The ICT Administrator will monitor the data from the filtering software to insure appropriate levels of safeguarding. Where there are causes for concern they will follow the school safeguarding procedures (see Safeguarding and Child Procedures) to refer that matter to the Safeguarding Designated Lead, the Headteacher will also be informed.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Protecting personal data

- Personal data used by the school will be recorded, processed, transferred within the legal framework of the Data Protection Act.
- Pupils are advised not to share personal information about themselves on the internet. They are taught about the associated risks and how to protect personal data.

Using websites with pupils

Pupils are often directed to internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing electronic world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- Sites used in school will be accessed as part of educational activities only. The selection of sites will be altered to reflect the ages and abilities of the pupils. Staff will review sites before they are first used to determine whether they are relevant and safe.
- All sites will be filtered via the school systems to minimize the risk of inappropriate material being accessed.
- If pupils are asked to make online accounts for access to materials, identifiable personal information will not be disclosed and only school e-mails will be used.
- The school will be as open as possible about the sites and software it uses and welcome parents who wish to raise concerns or understand more about the way that ICT/computing contributes to education.

Authorising internet access

- All staff must read and sign the ‘Responsible ICT Use Agreement for Staff’ before using any school ICT resource. Differing versions of this agreement may be used to match the personal and professional roles of staff members. A copy of this agreement will be given to staff members for their reference.
- All pupils will be introduced to the ‘Responsible ICT Use Agreement for Pupils’ and the reasons for the rules will be explained to them. Pupils will be expected to abide by the agreement. The school may decide to use different versions of this agreement to match the age group of the youngsters involved.
- Parents will be asked to sign and return a consent form alongside the pupil’s responsible use agreement. An additional copy of the agreement will be available to pupils within their yearly planner.
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date. This will take account of changes such as a member of staff who has left the school or a pupil whose access has been withdrawn.

Assessing risks

- The school will take all reasonable precautions to ensure that users abide by the acceptable use agreements and access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school can accept liability for any material accessed, or any consequences of Internet access
- The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use agreements which are published for their protection.
- The ICT administrator will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the ICT administrator and a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher/Nursery Manager
- Complaints of a child protection nature must be dealt with in accordance with School’s safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Introducing the e-Safety Policy to Children

- E-safety rules will be posted in all networked rooms and discussed with pupils at appropriate times throughout the school year. They will be in line with the policy and acceptable use agreements.
- Pupils will be informed that network and internet use will be monitored.
- By KS3, pupils will have received and continue to receive advice on the specific dangers and threats through a series of input (assemblies, community curriculum, ICT curriculum etc) in order to develop a toolbox approach to keeping themselves safe. However, due to the SEND status of some of our pupils it will be necessary to reinforce the messages repeatedly and ensure that pupils demonstrate a safe understanding.
- Pupils are required to hand in mobile phones at the start of each day and collect them at ‘signing out’. Some pupils have permission to use personal tablets and laptops for their work in school. We ask parents to sign an agreement that suitable parental controls are installed on tablets which are 3G / 4G enabled.

Staff and the e-Safety Policy

- A copy of the e-Safety Policy will be shown to all new staff and a copy will be kept in the staff policy folder and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents/carers attention will be drawn to the e-Safety Policy in newsletters, brochures and via the school website.
- Parents are asked to install parental controls on 3G / 4G devices that brought into school. There is a 3G / 4G agreement which parents must have signed before these devices are allowed in school.
- Schools may decide to hold meetings to brief parents about e-safety policies and concerns.
- Opportunities to address parents at events such as the Prize Giving and Christmas Shows may be used by the Headteacher to reinforce the message about e-Safety to parents.

Teaching e-Safety

E-Safety is embedded in the ICT curriculum – each lesson has opportunities for helping pupils to assess the risks of using online resources and social media. There are also age-appropriate specific e-Safety topics built into the Schemes of Work for ICT.

This curriculum teaching of ICT is complemented by input in assemblies and specific Community sessions. Both in-house and external visitor presentations are given and opportunities for pupils to discuss issues, their own experiences, etc.
All subject teachers using technology in the delivery of their subjects should be aware of this policy and the need to both monitor pupil use of the internet in their lessons as well as assisting pupils to discern suitable sources of information when setting homework tasks that require research, etc.

This reinforcement and monitoring in lessons is particularly important when pupils are using their own personal devices (laptops and tablets) in school. Although when connected to the school network such devices will have the same filtering as school PCs, staff need to be aware that some devices may be able to connect to the internet via mobile 3G and 4G networks which are unfiltered and which the school cannot monitor electronically. However, parents are asked to install parental controls on 3G / 4G devices that brought into school. There is a 3G / 4G agreement which parents must have signed before these devices are allowed in school.

Developing Strategy

Technology is changing at an unprecedented rate and it is important that our e-Safety strategy is constantly reviewed and updated to reflect these changes.

This policy will be reviewed at least every 12 months and whenever new information is available, such as when staff have attended e-Safety briefings or training or new guidance is released.

Created:	January 2016
Updated:	September 2016
Reviewed:	September 2017
Reviewed:	September 2018
To be reviewed:	September 2019