





## E-SAFETY POLICY

<b>Date Reviewed</b>	14 <sup>th</sup> December 2023
<b>Signed Headteacher</b>	
<b>Signed Chair of Curriculum &amp; Standards</b>	
<b>Date Revised</b>	Autumn Term 2024

**At Rednal Hill Infant School we will develop the learning environment to provide a range of Computing opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning, in line with our school's vision.**

**This Policy is to be read in conjunction with the Code of Conduct Policy, anti-bullying, acceptable use and the Child Protection Policy.**

*E-Safety Officer: Helen Drinkwater  
Network Manager: Entrust Technician*

### **Why is Internet use Important?**

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

### **How does Internet use Benefit Education?**

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries; maps and an infinite bank of knowledge
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

### **How can Internet use Enhance Learning?**

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity. Such as, the use of websites, email, blogs, podcasts, downloads and virtual learning platforms.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### **Authorised Internet Access**

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable Computer Use Agreement' before using any school 'computer' resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- As part of our school induction pack parents will be informed about children accessing the internet during the school day and to contact Anna Pendleton if they wish to share concerns or to discuss it further.

## **Internet**

- Rednal Hill Infant School uses Entrust Education Technologies "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material. The school will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk Via Helen Drinkwater or Entrust Technician and to Anna Pendleton.
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Securus Digital Monitoring is used on all Network computers in School and Staff Laptops.

## **E-Safety Policy**

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate our pupils about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Rednal's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Curriculum, Data Protection and Security, acceptable use and anti-bullying policy.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school computer systems, both in and out of 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 out of school, but is linked to membership of the school.

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.

## **School e-Safety Policy**

Our e-Safety Policy has been written by the school, building on Birmingham City Council guidance. It has been agreed by the senior management team and approved by governors.

## **Good Habits**

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

- Responsible use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from Birmingham County Council and Policy central including the effective management of content filtering.

#### **Governors:**

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

#### **Headteacher and Senior Leaders:**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-Safety Coordinator, Helen Drinkwater. The Network Manager role is provided by Denise Brooke (School Business Manager) and Entrust Technician.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The rest of the Senior Leadership Team will receive regular updates regarding e-safety in school.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

#### **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
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff (please see education and training)
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, if informed by the Headteacher following Securus Digital Monitoring alert.
- meets regularly with SLT to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

#### **Network Manager:**

The Network Manager is responsible for ensuring:

- that the school's network infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are periodically changed

- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- ensures that we subscribe to Securus, a monitoring system from Entrust and it is working effectively

**Teaching and Support Staff are responsible for ensuring that:**

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices, including GDPR.
- they have read, understood and signed the school Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the e-Safety Officer, Helen Drinkwater
- digital communications with pupils should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- they monitor computing activities in lessons, extracurricular and extended school activities
- they are 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
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Designated person for child protection**

Should be trained in e-safety issues 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

Either inside or outside of school.

**Pupils:**



- are responsible for using the school computer systems in accordance with the Pupil Acceptable Use Policy, which will be shared with them age appropriate.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- 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

### **Parents / Carers:**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of computers than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters or website.

### **Policy Statements:**

#### **Education – pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

#### **E-Safety education will be provided in the following ways:**

- A planned e-safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of computers and new technologies in school and outside school
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Children will be reminded regularly of the school's rules for use of computer systems and the internet.
- Staff should act as good role models in their use of computers, the internet and mobile devices

Children with SEND could be at risk of increased vulnerability, staff should be extra vigilant when monitoring use and when discussing risks and current concerns.

#### **Education – parents / carers:**

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line experiences. Parents often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site,
- Parent information sessions during parents evening and school events.

**Education & Training – Staff:**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings
- The E-Safety Officer will provide advice, guidance and/or training as required to individuals as required

**Technical – infrastructure / equipment, filtering and monitoring:**

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

- School computer systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority e-Safety Policy and guidance
- Password for teaching staff's ipads and computers will be recorded and kept in the schools safe.
- Member of staff responsible for data and usage of device assigned to them.
- The "master / administrator" passwords for the school computing system, used by the Network Manager must also be available to the Headteacher and kept in the school safe.
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- The Headteacher regularly monitors and records the activity of users on the school computer systems and users are made aware of this in the Acceptable Use Policy.
- Any e-Safety issues need to be reported to the Headteacher immediately.



- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg supply or trainee teachers or visitors) onto the school system. In the case of Infrastructure Engineers, the Master/Administrator password will be taken from the school safe by the e-safety officer or Headteacher and given so that essential work may be carried out. The password will then be reset by the Network Manager at the next visit to school.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet only when safely encrypted or otherwise secured.
- Memory sticks to have resource-based information and must not contain children's data or information.

### **Curriculum:**

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of computers across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided.

### **Use of digital and video images - photographic, video:**

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. **Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without parent's permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This is kept in the school office.

#### **Use of e-mail:**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail. Staff must report immediately to the Headteacher and Technician.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

#### **Use of Social Networking:**

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.

Staff will be advised of the code of conduct and the use of social media, so to not bring the schools reputation into disrepute.

- Pupils will be advised the appropriate ages required for Social Networking sites and that they can be only used with a parent.
- Pupils should be advised not to place personal photos on any social network space.

#### **Staff must ensure that they:**

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices. When using school computers ensure that they are properly "logged-off" at the end of any session in which they are using personal data.
- The devices teachers use must be password protected. Memory sticks must not be used to store any information about the children.
- The device must offer approved virus and malware checking software
- Staff must update iPad and Surface Pro passwords which are stored in the school safe. Annually passwords to be updated in line with policy.

- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

**Responding to incidents of misuse:**

It is hoped that all members of the school community will be responsible users of computers, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If any apparent or actual misuse appears to involve illegal activity the Headteacher (Anna Pendleton) will be informed straight away and disciplinary action will be taken.

GDPR breaches will be responded to in partnership with the school DPO, Satswana, an established provider of the service to schools.

**Handling e-safety Complaints:**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.

