Redlands Primary School ICT POLICY

Rationale

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which may not be age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology and teach our children how to use ICT in a safe way. This policy, supported by the Acceptable Use Policies (AUP; see Appendix 1) for staff and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. Both this policy and the Acceptable Use Policies (for all staff and pupils- see Appendix 1) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by pupils or staff.

The Technologies

New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging

- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole school approach to the safe use of IT creating a safe IT learning environment includes three main elements at this school:

1. An effective range of technological tools which are filtered and monitored;

2. Policies and procedures, with clear roles and responsibilities;

3. A comprehensive E-Safety education programme for pupils, staff and parents.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head Teacher, ICT Lead, Admin team with the support of governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any E-Safety issues which may arise in classrooms on a daily basis. The responsibility for E-Safety has been designated to the computing/PSHE co-ordinator who works in partnership with the Head teacher.

Our ICT Coordinator ensures they keep up to date with E-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 degrees internet safety. The school's ICT Coordinators ensures the Head, Senior Leaders and Governors are updated as necessary. The school teacher's Smart rules and uses the materials to support children's understanding of keeping safe online (See Appendix 2)

Staff awareness

- All staff receive regular information and training on E-Safety issues in the form of in house training and meeting time.
- New staff receive information on the school's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.

- Concerns are raised by staff as soon as incidents occur and are reported directly to the school's designated safeguarding team. Incidents should be recorded on a Child Alert form. All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Internet:

1. Redlands Primary School use a filtered Internet Service, which minimises the chances of pupils encountering undesirable material.

2. Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.

3. Staff should email school-related information using their Microsoft 365 address and not personal accounts.

4. Staff will preview any websites before recommending to pupils.

5. Internet searches are conducted using the Safe Search homepage found at http://www.safesearchkids.com/.

6. If internet research is set for homework, specific sites will be suggested that have previously been checked by the Teacher.

7. E-Safety information is found on the school website as well as links to CEOPs website.

8. If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the Headteacher, Administration support, ICT co-ordinator detailing the device and username. The filter can then be investigated and improved further.

9. Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.

10. Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a Teacher and then the ICT Co-ordinator so that the Service Provider can block further access to the site.

11. Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.

12. They are taught the rules of etiquette in email and are expected to follow them.

13. SMART rules are followed and no personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

14. Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.

15. A summary of these IT rules (SMART RULES) are displayed in the IT suite and all areas with IT resources. Pupils will be asked to sign to this agreement, ensuring that they are aware of expectations. (See Appendix). Copies of the agreement will also be distributed to Parents alongside the home/school agreement to ensure that key messages are reinforced at home.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Please refer to the laptop loan agreement that all staff are required to sign for more information.

Mobile Technology:

- Mobile technology for pupil use, such as Nexus 7s, iPads and netbooks, cameras are stored in a locked Safe. Access to the laptops is available via the Admin team (i.e Charlotte Woulds).

Members of school staff (not visitors or children) and IT company (the school use to manage IT) should sign in/out the technologies before and after each use.

- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.

When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

- No personal devices belonging to staff or children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent.

Data storage:

- Staff are expected to save all data relating to their work to their laptop or on the school server using the VPN
- The school do not use removable media however if they are used (for the purposes of school- such as school photos- this need to be agreed with the Headteacher. If this is agreed we expect the Encryption of all removable devices (USB pen drives, CDs, portable drives)
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Management Team.

Social Networking Sites (see Social Media Policy for more information):

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or

gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.

- The Local Authority and the School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use. Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - or using social media to bully another individual; or posting images that are discriminatory or offensive or links to such content.

The School reserves the right to monitor staff internet usage. The School considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

Digital images:

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children.

- Ensure you are aware of the children whose parents/guardians have not given permission for their child's image to be used in school. An up to date list is kept in the school administrative office.

- When using children's images for any school activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-Safety education to pupils and parents:

- All staff working with children must share a collective responsibility to provide E-Safety education to pupils and to promote E-Safety in their own actions.

- Formally, an E-Safety education is provided by the objectives contained in the Computing unit plans for every area of work for each year group. Even if E-Safety is not relevant to the area of IT being taught, it is important to have this as a 'constant' in the Computing curriculum.

- Informally, a talking culture is encouraged in classrooms which allows E-Safety issues to be addressed as and when they arise.

- The Computing Coordinator will lead an assembly on E-safety, including on Safer Internet Day, highlighting relevant E-Safety issues and promoting safe use of technologies.

- Staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the computing Coordinator with responsibility for E-Safety.

- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines. (See Appendix1)

- Parents/carers will be invited to attend an E-Safety awareness workshop once per year, run by the Computing Co-ordinator.

Maintaining the security of the school IT Network:

An IT company i.e. Tri computing, is appointed to maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However it is also the responsibility of the IT users to uphold the security and integrity of the network.

Complaints procedure:

Complaints will follow the school's complaints procedure and policy.

Monitoring:

The Head Teacher or other authorised members of staff may inspect or monitor any IT equipment owned or leased by the school at any time without prior notice. Monitoring includes: intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, email, texts or image) involving employees without consent, to the extent permitted by law. This may be to

confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School IT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches of Policy:

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings. Incident Report All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's Designated Safeguarding Officers or Head teacher.

Redlands Primary School

IT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from E-Safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will password protect all school devices or systems.
- I will not disclose my password to anybody else, or use search engines to save any to file.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time without pupils.
- I will report any E-Safety concerns to the Designated Safeguarding Officer/Headteacher and Administration Officer immediately.
- Mobile phones will be out of sight and switched to silent.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's E-Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.

I understand the procedures and agree to follow them with immediate effect.

Print Name: _____ Signed: _____

Date: _____

Appendix 1

Redlands Primary School
Pupil Acceptable Use

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

- I will only use IT in school for school purposes.
- I will ask permission from a member of staff before using the Internet and will only be online when an adult is in the room.
- I will only use my login and password and never share these with others.
- I will ask permission before bringing in memory sticks or CD ROMs into school.
- I will only open and delete my own files.
- I will not download or delete any APPS on the iPad.
- I will ensure I use the technologies carefully, never removing the iPads from the case or running with one.
- The messages I send will be polite and sensible.
- I will never give out my own or other people's name, address or phone number online.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away.
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my E-Safety.

Pupil Signed: _____ Date:_____

Class: _____

Redlands Laptop loan agreement

Following consultations on the allocation of computers under the DfE laptops for Teachers initiative, it has been recommended that a laptop be loaned to you while you remain employed at the school. While the laptop is in your care, you must abide by the following;

1. The laptop and peripherals it is issued with remains the property of Redlands Primary School and is only for the use of member of staff it is issued to.

2. Insurance cover provides protection from the standard risks but excludes accidental damage and theft from an unattended car. If the laptop is stolen from an unattended car, you will be responsible for its replacement.

3. Only software licensed by the school and approved by IT Support and the Head teacher are installed. Any other software that is required must be authorised. Any pirated or unlicensed software that is installed will result in action taken against that member of staff it has been assigned to.

4. It is your responsibility to bring in the laptop on a weekly basis and connect it to the schools network so that it can receive updates from the schools server. Not doing so will result in login issues and leaving the laptop vulnerable from external threats such as viruses.

5. Any internet charges incurred by staff accessing the internet from home whilst using the laptop are not chargeable to the school.

6. Any internet content that is accessed whilst connected to the school's network is monitored through a proxy server. Social networking, chat rooms and adult content are some of the categories that are strictly prohibited in a work environment as well as protecting the safety of the children during IT lessons. If any of these restricted categories are accessed offsite the member of staff will be held responsible and if found guilty, appropriate action will be taken.

7. Should any faults occur with the laptop or its peripherals, IT support must be informed as soon as possible to ensure that they can undertake any necessary repairs. Under no circumstances should the staff attempt to fix any suspected faults with the laptop or its peripherals.

8. If any member of staff needs help in operating either the hardware or software that comes with the laptop then please contact IT support. Training can be provided to ensure that teaching whilst using the laptop doesn't get affected.

9. The schools policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to

Please read the above carefully and sign below:

Failure to take reasonable care or abide by the conditions listed in this document may result in the Laptop being reclaimed and the person responsible for replacing the item.

I have read, understand and agree to abide by the terms of the Redlands Primary School **Laptop Loan Agreement.**

Signature: ……

Please Print Name: ……

Date: ……

iPAD/Tablet loan agreement

User Responsibilities

- The iPad screen is made of delicate glass, therefore it can be subject to cracking and breaking if misused; never drop or place heavy objects (books, laptops etc) on the iPad.
- The iPad has a case for its own protection, it should not be taken out of it nor should it be covered in stickers or unnecessary sticky notes.
- A microfiber cloth and approved laptop cleaning fluid should be used to clean the iPad.
- Do not subject the iPad to extremes of temperature as it can cause irreparable damage.
- The whereabouts of the iPad must be known at all times.
- It is the user's responsibility to keep the iPad as safe and secure as possible when not in use by applying a passcode and locking it away using the safe's provided in the classroom.

Safeguarding

- Users may not take photos of any other person without that persons consent.
- Photographs of children must be in line with the schools safeguarding policy.
- Images of other people may only be made with the permission of the person, or the parents of the person in the photograph.

Prohibited Uses

- The iPad/Tablet is a tool designed to enhance the learning for children. The classroom iPads should only be used for work-related purposes. *(Applies to teachers)*
- The classroom iPads should not be used for personal interests e.g. games and videos (unless these are educational related apps). *(Applies to teachers)*
- Social networking such as Facebook and Twitter are strictly prohibited when using the schools internet on premises.
- Internet content is monitored through the school's proxy. Any inappropriate websites will be flagged and is subject to the school's ICT policy and data breech.

iPad/Tablet Settings

- The iPad(s) you have been assigned to has a specific number and name for a reason. This should not be changed under any circumstances as it is required by the server.
- Apps can only be installed by the IT company (TRI) hence you will need to raise this with the Administration support
- Your assigned work email should only be used to download apps onto the iPad. As the iPad/Tablet is school property it is strictly prohibited to use your personal email.
- iCloud is not allowed. You should not be using either a work or personal email for this service as it can cause problems when resetting the iPad for a different member of staff.
- It is your responsibility to keep the iPad up-to-date. When updates become available it is pretty self-explanatory and in doing so you protect the iPad from any software vulnerabilities.

iPad/Tablet Equipment

- All iPads/tablets are issued with a USB cable, cover and charger.
- iPad(s), cover(s), USB cable(s) and charger(s) should remain with the iPad(s) it came with.

Lost, Damaged or Stolen

- If the iPad/Tablet is lost, stolen or damaged, the Headteacher and School Administrator must be informed immediately so that the relevant action can be taken.
- Users should not be lending or giving any iPads/Tablets and its peripherals to other staff as they will be liable should anything happen to the iPad and its equipment. This may result in a charge being incurred.

I have read, understand and agree to abide by the terms of the Redlands Primary School **iPad/Tablet Loan Agreement.**

Signature: ……

Please Print Name: ……

Date: ……

Appendix 2


Be Smart on the internet
Childnet International
www.kidsmart.org.uk
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
www.kidsmart.org.uk
KIDSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.