Federation of Riders Infant and Junior School

ICT Policy June 2017

Introduction

This policy aims to cover the different elements that Information Communication Technology (ICT) can cover within our school. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these to go ahead. This policy will set out a framework for how ICT will be taught, assessed and monitored throughout the school and should reflect the ethos and philosophy of our school. This policy has been written with guidance and support from other teachers, schools and local authorities. Often, schools will have a number of policies including E-safety and Social Media, but as a school we have decided to combine them into one policy. Further information on the different systems in school will be made available to staff online through the school's website and Google Apps account, this will be referred to as the ICT Handbook.

This policy should be read in conjunction with other school policies including Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection, Copyright Protection and Freedom of Information policies.

Aims/Rationale

ICT encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent, independent users and learners of ICT we aim:

- To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use ICT to help improve standards in all subjects across the curriculum
- To develop the ICT competence and skills of pupils through ICT lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use ICT to its full potential in all aspects of school life
- To use ICT as a form of communication with parents, pupils and the wider community

Curriculum – Computing and ICT across other subjects

In the 2014 National Curriculum, the subject of "ICT" was replaced by the subject "Computing". In this policy, *Computing* will refer to the specific lessons where skills are taught but when it is applied across the curriculum in other subject areas, it will be referred to as *ICT*. ICT will be taught across the curriculum and wherever possible, integrated into other subjects. There may be a need for stand-alone or blocked Computing sessions to teach skills that can then be applied in the cross-curricular lessons. Children will be taught ICT using laptops, tablets and a range of other devices.

The long term ICT map will show the journey in which the children are expected to take but this will be adapted each year to ensure that it is relevant and up-to-date. There will be a selection of age-appropriate ideas on the website with links to lesson plans, how-to guides and examples to ensure teachers are able to fulfil the curriculum. The ICT Leader will ensure that the plans provide coverage of what is expected and will ensure that the children are challenged and are able to succeed.

In Reception, children will be taught how to use various pieces of ICT equipment, including tablets, in accordance to the Early Learning Goals appropriate for them.

E-Safety for pupils

At Riders we take E-safety very seriously. We will ensure that it is taught often throughout the children's ICT and PSHE lessons as necessary. We will also provide children with dedicated e-safety lessons where appropriate and take part in annual events such as *Safer Internet Day* each March. All e-safety lesson plans and resources will be made available on the school website for parents to view. These will be reviewed regularly to ensure that they are up-to-date and reflect current needs. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have e-safety focussed parent meetings and will provide regular updates via our website and newsletters as appropriate.

All children will be taught about the Acceptable Use Policy (AUP) and will sign a copy related to their age phase. These will be stored by the ICT Leader. All staff will also complete an AUP.

E-safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online.

If there is a website available to children that staff or children deem inappropriate, they can either complete the form on our website or speak to the ICT Leader who will then contact Hampshire LA or use the Flexible Filtering service to block this in school.

If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the ICT Leader and executive head teacher and recorded as appropriate.

If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the ICT Leader who will investigate.

On all school blogs, the website and on Airhead, children will be provided with a button/page to report a problem to the ICT Leader should they find something inappropriate. Problems can be processed via an online form that is delivered immediately to the ICT Leader who can then decide the best cause of action.

Equal opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the ICT curriculum throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve.

If devices are provided by external sources e.g. for a specific child, the ICT Leader will need to be informed. He can then liaise with Agile ICT to ensure that it is suitable for use on our network.

Roles and Responsibilities - Senior Leadership Team

The executive head teacher and other members of the senior leadership team are responsible for monitoring the teaching of ICT throughout the school. The senior leadership team should decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, ICT action plans and timescales. They should also ensure that the ICT Leader and teachers are following their roles as listed below and in accordance to job specifications and performance management targets.

Roles and Responsibilities - ICT Leader

The ICT Leader will oversee planning in all year groups throughout the school and be responsible for raising standards in ICT. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The ICT Leader is responsible for overseeing the assessment of ICT across the school and providing opportunities to moderate ICT ability. They are responsible for keeping the hardware inventory up-to-date and ensuring the school has the appropriate number, and level, of software licenses for all software within the school. The ICT Leader is responsible for managing equipment and providing guidance for future purchasing. The ICT Leader is also responsible for ensuring policies, systems and procedures are sustainable.

Roles and Responsibilities - Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach ICT and to use ICT within their class. This will be in accordance to the schemes of work provided by the ICT Leader. They will also assist in the monitoring and recording of pupil progress in ICT. Teachers should also respond to, and report, and e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below.

Whilst checking of personal sites, e.g. email, is permitted during non-contact times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and ensure they are logged off appropriately (of both the website and their computer). Staff should follow, and agree to, the Acceptable Usage Policy below.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and ICT can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using ICT and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events. A range of e-safety websites, and our e-safety planning, will be made available on the school website.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities - Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher or the ICT Leader.

Hardware and software

Teaching staff are given a laptop to enable them to work at home and to access the server. The make, model number and serial number will all be recorded on the ICT Inventory kept by the LCT Leader. Other members of staff, such as Learning Support Assistants, may request a laptop to help with their role. There will be times throughout the year when the ICT Leader may recall the laptops to ensure that their virus protection is up-to-date.

When a member of staff leaves, they are expected to hand the equipment back to the ICT Leader who will ensure that the inventory is updated.

Each class has a computer attached to the interactive whiteboard to enable the teachers to present from. These are desktop PCs and will stay in the classrooms. Each year group also has a number of laptops and tablets that the children can use to access the curriculum. These are also recorded on the inventory.

Hardware should not be installed without the permission of the ICT Leader. If staff use memory sticks then the school's antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP.

The school uses ESET antivirus protection on all windows-based machines. This is maintained by Agile ICT and updated regularly. The chromebooks do not have virus protection as they are web-based only.

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information on to personal devices or memory sticks unless strictly necessary. This data should then be removed as soon as possible. When using a personal laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display e.g. in a parked car. This is less of a security threat with school laptops where remote access is used, as the data is not stored on the laptop itself.

There are a number of photocopiers and printers located across both schools. These can be used by any member of staff from a Windows-based machine. Pupils in the junior school will have access to the main Junior photocopier. They will be limited to 10 copies/printouts per day. The photocopiers are under contract and maintained by Sharp.

There are also a number of standalone printers for specific people and uses, such as in the SEN office.

The school will ensure that Display Screen Equipment assessments are undertaken in accordance with the Health and Safety Policy.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If users are unsure, they should speak to the ICT Leader for advice. The school reserves the right to examine or delete any files that are held on its system. If software needs to be installed, this be decided by the ICT Leader and he will liaise with Agile ICT if necessary.

The school's internet service is provided by Hampshire LA on a three-year contract. This is due for renewal in March 2017. This covers access to a variety of Hampshire services including Flexible Filtering which gives the school the ability to block or allow certain websites.

Access to the network

Staff will be issued a username for the network when they join consisting of first initial and surname e.g. John Smith would be jsmith. A default password will be set and it is the teacher's responsibility to ensure that this is changed and kept secure. Staff are also able to access the server remotely from home. This is known as Remote Working. Staff will be issued with guidance of how to use this and how to ensure that it is managed securely. Pupils will not have access to this.

Pupils in Year 1 and Year 2 will not require a log-on and will be able to access the chromebook laptops via an automatic signing in process. When pupils join the Junior School, they will be issued with a login to access the chromebooks. This will take the format of first initial and then the first four letters of the surname e.g. John Smith would be jsmit@ridersapps.co.uk

In the case of any duplicates, a number will be added to the end of the username. A list of all duplicated accounts will be created by the ICT Leader and passed to all staff at the start of the school year.

Pupils will not be given specific access to the school network as everything they use will be online.

The school has a Meru wireless network. The WiFi password for this is available for staff on request. Staff may connect their own laptops to this network providing that the ICT Leader has checked the laptop for sufficient virus protection software. If the password is provided on paper, it should be destroyed once it has been used.

General internet and email access for staff and pupils

Where appropriate, staff may be given a school email address and access to SIMs. This is the email that staff should be using for professional communication. Upon joining, staff will be added to the mailing lists for staff in either the infant or junior schools. This will ensure that they receive communications that are sent out. The password for this SIMs/Email account must be changed every 4 months and previous passwords may not be re-used in accordance with Hampshire's ICT Policy.

The internet may be accessed by staff and by children throughout their hours in school. We ask that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended.

The teaching of email and internet use will be covered within the ICT curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

Pupils entering Key Stage 2 will receive an email address when they first use the chromebooks and this should be monitored by the class teacher and the ICT Leader.

All staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the ICT Leader so it is the user's responsibility to ensure they log off appropriately. If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the ICT Leader who will investigate.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to the ICT Leader using the web-form provided on the school website or by discussing this with their class teacher.

Users of the network must not create, download or upload material that is designed or would be likely to annoy, harass, bully or inconvenience others.

Due to the potential impact on the school system and on other users, the use of streaming media such as video or audio should be kept to a minimum. Streaming should be limited to short clips only. Staff members should not stream TV, films or continual broadcasts (e.g. sports events or news) during school hours.

The internet and filtering is provided by the local authority and the ICT Leader will run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by the local authority. Additional sites can be enabled by the ICT Leader and a record will also be kept of the sites enabled by school. It is not possible to block certain aspects of a site e.g. a video on YouTube so care needs to be taken when children are accessing the internet.

Google Apps and other online services

The school uses a variety of different online services to aid in the delivery of the curriculum. Many of these provide accounts for pupils. Where possible, the school will try to streamline the process to make logging on, and the managing of usernames, as simple as can be.

The main online learning will take place on devices known as chromebooks and these will access the Google Apps environment. This provides tools such as word processing, presentations and email. Google stores data about its users in accordance with the Safe Harbour Agreement.

We also make use of a system called Airhead which is an online portal connecting other services together. Most services will require a username in the same format as for the chromebooks. If this differs, children and staff will be made aware.

The following tools currently require a username and password: J2E, Purple Mash, Sumdog, Accelrated Reader, Times Table Rockstars, Education City and Google Apps. These are mostly used in Key Stage 2 only.

There are many online services around the world that follow COPPA guidelines which state that users under the age of 13 should not have accounts as it is illegal in the United States to collect data (including names) on children under 13. However, these laws do not always apply in the United Kingdom and the main account holder for all of these systems will be the ICT Leader. The children will be accessing resources that are deemed appropriate by the ICT Leader.

Passwords

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

For online services mentioned in school, such as those listed above, pupils may not have the ability to change their password as this is done centrally by the administrator which will usually be the ICT Leader. If there are issues, children or staff should speak to the ICT Leader for assistance.

There are some services where a “school password” has been used. This is known by staff and should be kept secure. It is important that these usernames and passwords are not given to children to use.

Children will be taught about acceptable passwords and the need for a secure password and this will form part of the ICT curriculum as they progress throughout the school. Teachers may choose to keep a record of the passwords in their class if they wish. Teachers will also be shown how to reset passwords for Google Apps accounts.

Technical support

Minor issues are dealt with by the ICT Leader or staff as appropriate. Additional hardware support is provided as and when necessary by Agile ICT either as part of scheduled on-site visits or by remote support. Support for the website is provided by Agile ICT. Additional office-based support (e.g. SIMs) is provided by the Hampshire IT Helpdesk and forms part of the annual Service Level Agreement that the school has in place.

School transfers and transition

When children join the school, a member of the office staff will provide their name, year group and class to the ICT Leader so that he can create logins for the services as listed above. This will usually take place within a few days and class teachers will be emailed when it has been completed.

When a child leaves, if they wish to export their data from Google Apps, they need to inform their class teacher and the school will organise to download it and pass it on either via email or on a CD or memory stick. It is not possible to export scores and rewards from many of the online services listed above. At the end of a school year, any children that have left during that academic year will have their details deleted from the services listed above.

When a member of staff leaves, they should speak to the ICT Leader if they are unsure about how to transfer their files to a different device. Their accounts will be removed when they are no longer needed.

Backing up data

The network and server are backed up using a service called Agile Vault provided by Agile ICT. There are three layers of backup across two completely separate hardware and physical locations:

1) Shadow Copy – runs twice a day at 7:00 am and midday

2) Replication to the Agile RMB (replicates every 5 minutes)

3) Remote backup to the Agile Vault Backup Servers at the Agile ICT office

For individual files or folders on the network, these can be restored using a tool in Windows Server to recover previous versions or by using a tool on the server to reload the file from the shadow copy. These shadow copies are kept for 100 days.

In the event of the server malfunction, the school can contact Agile who will transfer us to our back-up server known as the RMB. This will look and behave exactly as the server would, but with less speed or processing power. This RMB is setup to ensure that critical users e.g. office and staff can continue using the network and accessing files but is not sufficient enough for hundreds of users. As our network is not configured in this way and all children access their learning on the internet rather than the server, this should not impact them too much enabling lessons to continue.

Agile advises that the worst-case scenario is that any data created between the last replication to the RMB and the server malfunctioning would be lost although this would only be five minutes' worth of data.

We have an agreement as part of Agile Vault backup that Agile will repair or replace the server as soon as possible. Once the new hardware is in place, data from the RMB would be copied to the new/repaired server.

Google Apps is not backed up, but being a cloud solution, this means it is always available should users need access to their documents.

School website and Blogs

The school website consists of different components that will need to be updated regularly, termly or annually. Content such as diary dates and newsletters will be updated by the office staff as and when they are available. Policies will be uploaded by the ICT Leader once they are ready to be shared. Other content e.g. curriculum or staffing information will be edited when necessary.

The school uses blogs to share learning with parents, children and the wider world. These blog pages are public and it is expected that these will be updated by staff at least fortnightly. Children have access to add content but this must be approved by a teacher before it goes live. Visitors to the blog may also leave comments but these will not be seen by children or go live on the site until approved by a teacher. Spam messages (often containing inappropriate links and language) are caught by software installed on the blog (akismet) and this is monitored by the ICT Leader. This is also updated regularly.

All blog posts will automatically be published on the school's Twitter feed (@ridersschools) which is managed by the ICT Leader.

Sustainability and environmental impact / disposal of hardware

To ensure that the level of ICT across the school is sustainable, the ICT Leader is responsible for the upkeep of the ICT Handbook which will contain usernames, passwords and guides to online tools and software as well as details of licenses and a complete ICT Inventory of all equipment.

Hardware is disposed of safely and securely through a local company, Jamie's Computers, who are approved by Hampshire LA. They will wipe the devices and then either dispose of them or sell them with proceeds going to charity. The school will receive a certificate of disposal a few weeks after collection. These devices will also be moved to a separate section of the inventory to keep track of disposals.

Responding to unacceptable use by staff and pupils

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time. Records of these incidents will also be kept by the ICT Leader.

Use of mobile phones and handheld devices by staff

Each class has been issued with a class tablet for the purpose of taking photos and for blogging. There are also a number of tablets in each year group that can also be used for the same purpose. This should cut down on the need for staff to use their own devices within school.

Staff may attempt to connect their phone to the school's wireless network in accordance with the network guidelines in the ICT Handbook but should be aware that this may not work due to the settings available on their phones.

Staff should not take photos of children on their mobile devices. If photos are taken, for example if no other camera is available on a school visit, then staff should make sure that these photos are in line with the school's photo use procedure as outlined below and that they are transferred to the school network as soon as possible. These should also be removed from the staff devices and any other online backup service e.g. Google Photos or iCloud that the staff member may have setup on their phone.

Use of digital videos and images

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will try to ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award or is appearing in the press
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities or getting changed for PE
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the ICT Leader. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online

If staff use personal cameras or phones to take photographs of children within school, these should be removed from the device as soon as possible. We are fully aware that this is necessary at times, but precautions should be taken to minimise the risks.

Social Media

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community (such as children's parents) and just ask that these members of staff take extra precaution when posting online
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening
- Not use these media to discuss confidential information or to discuss specific children
- Check with the ICT Leader if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.

As a school we will use our website, a mobile app and Facebook to post information. These posts can only be sent by the office staff or the Senior Leadership Team. If other members of staff wish to send a post via one of these services, they should contact an approved user first. The use of the Facebook group will be monitored and we will ensure that we block any followers that appear inappropriate.

Staff are reminded that all communication with parents whether it be face-to-face, via email, telephone or online should be kept professional at all times.

Some teachers may decide to explore other uses of social media e.g. Instagram, to share learning from their class. If this is the case, the ICT Leader should be kept informed.

Copyright and Intellectual property right – e.g use of copyright-free images

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the internet. They will have discussions about the proper use of images with questions such as 'Is it OK to use an image we find online?' As they progress through the school some children will start referencing the sites they have used in their work. This could be as simple as putting the name of the site the image came from or a hyperlink. It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the internet without some thought on their use.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This is in accordance with guidelines laid out by the local authority.

Complaints

Incidents regarding the misuse of the Internet by students will be delegated to the ICT Leader who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the executive head teacher. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

Acceptable Usage Policy – Staff and Visitors

This document has been written to ensure that staff and visitors use the ICT throughout the school appropriately. If they have any questions regarding this policy, they should direct them to Senior Leadership team or the ICT Leader.

Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that they have a sensible password
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer – particularly in shared areas
- Make use of resources such as tablets or cameras but ensure that these are returned after their use. They should also endeavour to remove pictures/files regularly
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the ICT Policy
- Be aware that software or hardware should not be installed without prior consent of the ICT Leader
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the executive head teacher
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
- Where staff are using their own digital equipment such as cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible;
- Report any issues to the Senior Leadership team or ICT Leader as soon as possible
- Return any hardware or equipment if they are no longer employed by the school

Signed ______________________________ Print ____________________ Date _______________

Acceptable Usage Policy Junior School

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, tablets and cameras. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher or Mr Addison.

- At all times, I will think before I click (especially when deleting or printing)
- When using the internet, I will think about the websites I am accessing
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around the school.
- I will report any breakages to my teacher or Mr Addison as soon as I can
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

Signed (Pupil) ___________________________________ Class __________ Date _______________

Acceptable Usage Policy Infant School

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, tablets and cameras. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher or Mr Addison.

The Golden Rule: **Think before you click**

☺ I will be careful when going on the internet.

☺ I will only use the internet when a teacher is with me.

☺ I will tell a teacher if I see something that upsets me.

☺ I know people online might not be who they say they are.

☺ I will be polite when talking to people or writing online.

☺ I will think before I print or delete.

☺ I will be careful when using or carrying equipment.

☺ I will remember to keep water bottles away from the ICT equipment.

☺ I will keep passwords secret, but I can tell my family.

☹ I won't tell anyone any personal details like my phone number or last name.

☹ I won't logon using someone else's username.

Signed (Pupil) ____________________________________ Class __________ Date ________________