

Riverdale Primary School

Acceptable Use of ICT Policy

This Policy was initially produced in the Summer Term 2007 through a process of consultation with teaching staff from school and advisory staff from the LA. It was approved by the governing body in November 2007 after discussion in committee.

The implementation of the policy will be monitored by the Head Teacher and will be reviewed annually.

Next Review – Summer 2024

Review Date

Autumn 2018 No changes required

Autumn 2019 No changes required

Autumn 2020 No changes required

Autumn 2021 Change of MDM used in school JAMF

Summer 2022 Filtering provider & broadband updated alongside order of appendices

Summer 2023 No changes required

Who will write and review the policy?

Our school internet policy has been created by using information from BECTa, Redcar and Cleveland Local Authority and government guidance. It has been discussed by the whole staff and approved by governors, who realise how intrinsic to the running of the school, both at a management level and an educational level, the internet is.

Due to the nature and speed of ICT developments, this policy will be reviewed ANNUALLY, by the Head teacher and Senior Leadership Team.

Why have this policy?

The internet is now the most data rich source of information in the world. It can potentially “bring the world into the classroom.” From a teaching point of view this is an essential resource for planning and delivering lessons. From a child’s point of view it is an excellent source of information that enhances the personalised learning agenda.

The internet based school learning platform allows effective dissemination of specific information (notes, dates, files) to specific people (teachers, parents, staff). In addition to this, government expectation is that all pupils have access to a digital workspace since September 2008. This is a place to upload files that they have created and access appropriate resources. Increasingly the internet is becoming a place to share information, collaborate with others and our school would like utilise the learning platform to enhance the education of all children. Essentially this will be integral to most ways of working in the workplaces that they will eventually enter.

This policy seeks to ensure users know what good practice is and outlines steps and procedures that will be taken when the darker side of the internet shows itself.

Filtering

The school has a 30mb broadband connection which is provided by Virgin Media and is monitored and supported by One IT services and Solutions.

They work alongside Northern Grid and Securly (web/content filter)

To ensure filtering is appropriate and that where there are problems there are guidelines to follow. The filters at each stage are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments. However, when dealing with the internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined below have been taken.

Use of the web is monitored and traceable by One IT network administrators. All web activity is logged for 6 months. In addition to this is the consideration that children will inevitably access the internet outside of school. We therefore aim to educate them about internet safety, not simply cover their eyes.

As part of our ICT mobile device project we have 3 sites unblocked as an exception for our year 5 and 6 children. They are iTunes, One Drive and Youtube. These sites have been unblocked with the approval of the academy trust as an integral part of the school’s project.

When will pupils have direct access to the internet?

Children in all classes in school will have access to the internet.

However different types of use which are outlined below, will be used to enhance children’s safety within school:

* Online content (e.g., CBeebies) will often be used by the teachers for specific tasks. In these situations the children are not searching the internet or navigating away from the page/s and tasks that have been set. Teachers **will have previewed** the site to ensure that it matches the learning outcomes of the lesson/setting.
* Searchable cached sites such as Espresso will allow access within a site but not beyond it
* In most cases, to avoid fruitless hours of browsing, a key website/s will be identified by the teacher or ICT technician, for the children to use to find information. This can be made easier with the use of bookmarks on the platform or shared links on the School network.
* Children from Year 4 onwards will be able to use a safe search engine such as BING and BBC when searching for information.
* It is essential that access to navigate accidentally or purposefully away from the site or agreed sites isn’t possible. Children are never left unattended when searching the internet, with adults moving around children all the time whilst working. Random spot checks of children’s search history will also made.

This is not a failsafe way of preventing access to inappropriate sites but is a good line of defence and will stop access very quickly should the site load part way or fully up.

Children will not be allowed to access and search the internet unless authorised by a member of staff.

Responsibility for the monitoring of what the children find is then the responsibility of that adult. The school’s scheme of work/curriculum plan identifies when searching on the internet is appropriate to develop children’s ICT skills; other uses are the sole responsibility of the supervising adult.

Staff use of Internet

All staff must follow the acceptable internet use policy for staff laid out in Appendix 8, when accessing materials on the Internet.

Staff must only access the internet for personal reasons with prior agreement with the Head teacher and accessed outside of their direct supervision or teaching/preparation commitments.

**The use of the network for personal monetary profit or gambling is strictly forbidden.**

Use of email

Children

Children from Year 5 onwards will be given a “professional” email account. The account is set up using Microsoft Office 365 E-mail. The children are at liberty to use their accounts for correspondence between one another or a class of children from a different school organised by the Head teachers of both schools.

**They must ask a member of staff before using it to contact or reply to anyone else.**

**Use of personal email accounts in school is not permitted.**

Use of newsgroups or forums/chatrooms in school is not permitted

Staff

Staff will be given a “professional” email account. The account is set up using the Microsoft Office 365 E-mail.

The staff are at liberty to use their accounts for correspondence between one another or other professional bodies for professional purposes only.

Passwords must be changed by the user on a monthly basis.

Users agree through the staff agreement form to keep passwords secret, even from their family and friends.

**Use of personal email accounts in school is not permitted.**

Use of newsgroups or forums/chatrooms in school are permitted when located on a professional site

The staff internet/email agreement form sets out the terms and conditions that they must agree to adhere to **before** being allocated an account.

All school accounts will carry the tag:

This e-mail is confidential and privileged. If you are not the intended recipient please accept our apologies; please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful. Please inform us that this message has gone astray before deleting it. Thank you for your co-operation.

**Health and safety – Being Safe**

**Internet**

* Children will not be allowed to access and search the internet unless authorised by a member of staff.
* Appropriate behaviour and understanding of how addresses are composed will be explicitly taught before ever using an internet search in school and will be reinforced by visual reminders.
* Accessing and interacting with the internet is part and parcel of many users’ reasons for having an internet connection. Simply blocking the children from using internet it is not educating them f or the real world (and use at home). Therefore internet safety is implicitly taught from Reception every year as part our ICT/PSHE curriculum & also in a dedicated internet safety week annually. Safety on the internet will also be continually reinforced, whenever children are accessing the internet in school.

Key themes to be covered are listed below:

* Safe browsing on the internet
* Use of chatrooms
* Use of blogs/webspace
* Use of email
* Copyright
* What to do when you come across something that is inappropriate

# Internet and Email

* All children and parents/guardians will be required to agree to adhere to the conditions laid out in the home/school agreement for using the Internet and Email account provided by school, before they are able to use either.

Failure to adhere to these conditions may result in the internet facility and email account being removed from that child.

* All staff will be required to agree to adhere to the conditions laid out in the staff agreement form, for using the Internet and Email account provided by the school, before they are able to use either.

Failure to adhere to the agreement will result in formal disciplinary procedures.

# Email

* Users must report any inappropriate emails to the Head teacher.

* Users must report any attempts by people who they don’t know trying to contact them.
* Children will be taught to never give out their email address in a public setting (virtual or real) or divulge personal details in public internet space in Year 5 and 6, as part of the teaching of Internet Safety. This will be reinforced whenever the internet is used through continued verbal reference and visual reminders.
* In accordance with the Data Protection Act 1984/98, users are not allowed to access other user’s personal files and folders. The exception to this being system administrators who can gain access through permission from the Head teacher when just cause has been established.

The school has a policy on the use of photographs, images and videos of children. Majority of photographs are used for within school, however on occasions we are asked if images can be used by other parties on their websites or newsletters to promote the work they have done. Photographs of children that can be viewed by others other than in school, will only be ever be used after permission has been sought from parents.

Children must adhere to only taking photographs/videos of others with their permission.

Children must share with class teacher of any photos/videos they receive of inappropriate behaviour.

These statements will have been agreed to as part of the home/school agreement.

Wireless Network security

The school’s wireless network is encrypted by a WPA encryption key to prevent unauthorised access. It has been checked and authorised by the One IT network administration team. If a breach in security is discovered it will be reported to the Head teacher and steps will be taken to review the security level in place with relevant specialists.

Use of mobile devices

Mobile phones are not permitted to be used by children within school unless permission has been granted by the Head teacher. Failure to observe this will result in confiscation. If a child brings a mobile phone to school with them, it should be given in to their class teacher and locked away in a secure cupboard until the end of the school day. Children should then collect their mobile phones from their class teacher at the end of the day. Any mobile phones not collected will be locked in the secure cupboard overnight.

Mobile phones are permitted to be used to make or receive calls, send texts by members of staff, outside of their direct supervision or teaching commitments.

Staff should be aware to make sure conversations take place outside the earshot of parents and children.

During lesson and supervision times all mobile phones should be turned off or silent mode, and stored securely away from sight of children to avoid distractions within the class setting and children gaining access to the device.

If there is a specific reason to keep a mobile phone on for a limited time, staff may request permission for this from the headteacher or deputy in their absence.

Mobile devices issued by the school, and personal devices that have all content removed are allowed in school for year 5 and 6 children. They will connect to the Internet through the school’s filtered broadband connection. Children are allowed to connect their devices to other wireless providers either at home or in the community subject to them following the guidance given by the school.

Children are not at liberty to install software on to their devices.

The devices will be subject to random checks and any software or material found to be inappropriate will be deleted, and possible confiscation of their device.

All children will sign an ownership agreement form that sets out the terms and conditions of their use before they take the devices home.

When children/adults are using the mobile devices in school and any other digital device, they must ask permission to take an image of another person. Failure to adhere to the agreement will result in action being taken by the Head teacher.

A school device should be the preferred option to take photographs and videos.

The Head uses a school mobile phone to take photographs for the school Facebook & Twitter Account. The material is usually then deleted or uploaded to a school computer to be able to be used for display purposes in school.

If staff need to use a camera on their own mobile phone to take photographs or videos of students this should be saved on a school device and deleted from the personal device as soon as possible and no longer than 3 working days.

The school mobile phone may be used by the headteacher for personal use, as agreed by the governing body

Parents who have concerns or queries about use of mobile devices can contact their child s class teacher, who will assess whether the Head teacher needs to become involved. Steps will be taken to resolve issues where appropriate and lessons learned/implemented where relevant.

Moblie Device Management (MDM)

Our school uses JAMF MDM to effectively manage the profiles on our devices. The profile allocates app codes bought through the volume purchasing and distributes accordingly. Restrictions are also placed on the devices managed as a further level of security.

School Facebook Page

At Riverdale Primary we recognised the large numbers of parents and carers using Facebook as their chosen means to communicate. Our rationale was to create a Riverdale Primary school page where parents and carers can share successes and selected information regarding events, notices and achievements. Photo permissions are obtained for every child upon entry to school.

Our Facebook page is professionally managed by staff and open to the approved members from our school community. Content from this page can be re-shared. It is not linked to any personal Facebook accounts and staff are not permitted to link any personal account in conjunction with this account. This account is sanctioned by the Head teacher and monitored regularly.

Starters and Leavers

It is the responsibility of the office staff to inform the Computing leader/ Technician of any member of staff/pupils or governors joining or leaving the school. The staff/pupil/governor leaving will have to return all ICT equipment owned by the school to the Computing leader. The technician will then ensure that leavers’ access is removed, or disabled. All new starters, whether they are staff or pupil will need to have read, understood and signed the school acceptable use policy, before any will be granted access will be granted to any ICT equipment. All visitors requiring access to school ICT equipment need to sign the acceptable use policy. The school office supplies all new members of staff, students and supply teachers with the AUP form to read and sign as well as temporary log in details for the school network, only. When the new starter data has been entered in to SIMs then a more permanent log in will be issued to staff from the school network.

Reporting Incidents

A very important element of safeguarding is the ability to identify and deal with incidents. All staff and pupils have a responsibility to report online safety incidents so that they may be dealt with effectively. All incidents should be reported using the CPOMS system under the correct heading. Incidents must include the correct members of the online safety team and be action appropriately in order to generate a chronology on this new platform. Incidents will be dealt with in accordance with school policies

Other Areas of Teaching and Learning

Staff are required to print via the office photocopier, the data is transferred using the curriculum network. Teachers are required to input their unique year group ID code to access the printer. The printer default settings are sent to a ‘custom box’, this ensures that all printing is collected and the waste is reduced. Staff are required to input their name and the code, this will help staff identify their own printing when at the machine. The printing will be held in the photocopiers memory until the staff access this at the photocopier. The memory automatically clears in items for not printed within three days.

Parent involvement

Parents will be kept informed of relevant developments through the school’s newsletters, parents meetings, the school website and the Learning Platform.

Parents who are unhappy with aspects of ICT will be invited to follow the school’s complaints procedure.

School will always seek to discuss and try to accommodate parents’ religious beliefs which affect children’s ability to be able to access technology.

To ensure families do not feel discriminated against if they do not have access to a computer or internet.

* School will always provide paper versions of information and work home as well as putting them on the learning platform.
* School will actively promote places locally that offer free access to the Internet and the times they are available.

**Appendix 1**

Permitted Communications Summary

| Communication Technologies | Staff and Other Adults |  |  |  | Students/pupils |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school |  |  |  |  |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  |  |  |  |  |
| Use of mobile phones in social times |  |  |  |  |  |  |  |  |
| Taking photos on mobile phones/personal devices or other camera devices not owned by school |  |  |  |  |  |  |  |  |
| Taking photos on mobile phones/personal devices or other camera devices not owned by school |  |  |  |  |  |  |  |  |
| Use of hand held devices eg ipads/ipods |  |  |  |  |  |  |  |  |
| Use of personal email addresses in school or on school network |  |  |  |  |  |  |  |  |
| Use of school email for personal emails |  |  |  |  |  |  |  |  |
| **With e-safety training and in a professional capacity only …** |  |  |  |  |  |  |  |  |
| Use of chat rooms/faciltiies |  |  |  |  |  |  |  |  |
| Use of instant messaging |  |  |  |  |  |  |  |  |
| Use of social networking sites |  |  |  |  |  |  |  |  |
| Use of blogs |  |  |  |  |  |  |  |  |

**Appendix 2**

Users Permitted Actions Summary

Users shall not visit Internet sites, make posts, download, upload, data transfer, communicate or pass on materials, remarks, proposals or comments that contain or relate to :-

|  | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| --- | --- | --- | --- | --- | --- |
| Child sexual abuse images |  |  |  |  |  |
| Promotion or conduct of illegal acts |  |  |  |  |  |
| Adult material that potentially breaches the Absence Publication Act in the UK |  |  |  |  |  |
| Criminally racist material in the UK |  |  |  |  |  |
| Pornography |  |  |  |  |  |
| Promotion of any kind of discrimination |  |  |  |  |  |
| Promotion of racial or religious hatred |  |  |  |  |  |
| Threatening behaviour, including promotion of violence or mental harm |  |  |  |  |  |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  |  |  |
| Using school systems to run a private business |  |  |  |  |  |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by school |  |  |  |  |  |
|  |  |  |  |  |  |
| Uploading, downloading or transmitting commercial software or any copyrighted material belonging to third parties, without the necessary licensing permissions |  |  |  |  |  |
| Revealing or publicising confidential or propriety information |  |  |  |  |  |
| Creating or propagating computer viruses or other harmful files |  |  |  |  |  |
| Carrying out sustained or instantaneous high volume network traffic that causes network congestion and hinders others in their use of the Internet |  |  |  |  |  |
| On-line gaming (educational) |  |  |  |  |  |
| On-line gaming (non educational) |  |  |  |  |  |
| On-line gambling |  |  |  |  |  |
| On-line shopping/commerce for school use |  |  |  |  |  |
| File sharing |  |  |  |  |  |
| Use of social networking sites |  |  |  |  |  |
| Use of video broadcasting with adult guidance eg Youtube |  |  |  |  |  |
|  |  |  |  |  |  |



**Appendix 3**

**Parents/Carers**

I have read the school’s acceptable use policy for ICT

I have read the rules for acceptable use my child needs to follow and I agree to support my child to follow the rules given for acceptable use of his/her ipad

I understand the school owns the devices during the project and has the option to confiscate devices from any child that is not following the acceptable rules of the project.

Name of Child………………………………

Signature ………………………………. Date ……………………

Logo, company name

Description automatically generated

Logo, company name

Description automatically generated**Appendix 4**

**Acceptable Internet Use Policy For Children**

**Remember that we use the computers and the Internet for Learnin**g

* All children must have written permission from their parents or carers to use the internet
* Only access those services and sites that you have been given permission to use
* Do not use Internet chatrooms or social media networking sites, eg Facebook, Twitter, Movie Star Planet etc
* You may only use the internet when supervised by a teacher or other responsible adult
* Your use of the internet is restricted to activities that relate directly to your Academy work
* Do not reveal any personal information about yourself or any member of the academy , adult or child
* Do not engage in any online conversation or dialogue without the permission and supervision of the class teacher
* In any communication you should always be polite and considerate. The use of bad, offensive or aggressive language is not allowed
* If you see anything you are unhappy with or you receive messages you do not like, let a teacher or adult know immediately
* Remember that all your internet and email use is checked
* If you deliberately break these rules you will be banned from using the internet or computers at the academy

**Appendix 5**

**Home / School Agreement for the Acceptable Use of Hand Held Devices at Riverdale Primary School**

**Pupil**

I understand at school my iPad will be linked to the school internet.

• Only use websites which you are directed to. (Don’t go on inappropriate websites!)

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

• Only go on the internet when the teacher asks you.

• Always ask permission before taking a photo or video of another person.

• Always make sure your iPad is out of reach when the teacher is talking to avoid fiddling.

• Always ask permission before changing any settings on your iPad.

• Charge your iPad every night ready for learning the next day.

• Always use the charger it came with.

• Bring your iPad to school every day, as it is a vital learning tool.

• Make sure you only take videos and photos in an appropriate setting (e.g. not in a bathroom, bedroom etc)

• School is silent! (turn your volume off in school)

• Always remember to take your iPad home on a night.

• Only ever touch your own iPad. Only touch other devices if you have permission.

• Personalise your own iPad, with a screen saver and wallpaper appropriate for school.

• Keep all documentation in a safe place at home.

• When you are not using your iPad put it away in a safe place.

• Do not behave in a way that will cause damage to your iPad. (Take care not to swing or drop your iPad).

• Always send polite and responsible messages, messages will be monitored.

• I understand school will provide me with some key apps for my learning and I must not delete them, school also

provides a more secure network for me to access the internet than other wifi networks.

• The apps that are on my iPad are appropriate for my age and will not cause offense to others.

• Always ask an adult before downloading additional apps and make sure they are age appropriate.

• I understand social networking apps or websites are not permitted in school.

* I understand I must not access an alternate Apple ID on my mobile device or download anything off another Apple ID onto my device.

• The content on my iPad (e.g. apps, photos, notes, internet history) will be appropriate and not cause offence.

• I understand that my iPad is covered under your own insurance plan and school cannot be responsible for any

damage or lost.

• I understand I may lose functionality on my iPad after a certain time at night. I may also lose functionally at school

if teachers deem so.

• I understand my device will be linked to our school’s mobile device management system and school can view content on the device as well as enforce restrictions.

• I am clear that school retains the right to restrict any content deemed unsuitable.

• I am aware that my device will need to be configured by school, which includes a full reset of the device.

These are the steps you should follow when using your iPad, inside and outside of school. If it isn’t written above don’t do it!

You need to agree to follow these guidelines and those in our Internet and Computing Curriculum Policies, sign the form below.

Name of Child …………………………………………. Signed ………………………………….. Date ………………..

**Appendix 6**

Responding to incidents of misuse/error

As you are all aware we have a walled garden in school, which filters the websites which you and the children are al- lowed to access, for safety reasons. This system in not 100% guaranteed therefore we need to be aware of potential risks, for both children and adults.

There are procedures set out in the Online Safety policies in school to follow if such events arise. These are summarised below.

You need to:

• Immediately turn the screen off / put the device to sleep (pressing home/lock button)

• Leave the website on the computer/ device

• Report it to the Online Safety Team /HT immediately

• Log incident on CPOMS with required action and including appropriate staff

• If required it will then be investigated by the LA

• If required It will be investigated by our Internet provider

• If needs be then it will reported to the police.

**Just remember it is not yours or the children’s fault, but it does need dealing with!**

**This proceed should be followed and children in all classes should be made aware of it.**



**Appendix 7**

**Misuse of the Online Safety Policy**

If you find you or another member of staff have possibly not abided by the Online Safety policy and rules have been breached, then please follow the following procedures to rectify the problem.

* Seek advice from the Online Safety Team
* (Who will if necessary have an unofficial word with the Head Teacher)
* Word of advice (reminder if it continues) CONTINUAL ABUSE
* Computing Leader will refer the matter to the Head Teacher
* A meeting will take place with the Head Teacher and Computing Leader. Minutes of the meeting taken and monitored
* Formal investigation into continual abuse of the school policy

**CONTINED ABUSE**

* Trustees will be informed and disciplinary proceedings will commence



**Logo, company name

Description automatically generatedAppendix 8**

**Acceptable Internet Use Policy For staff**

**Remember that we use the computers and the Internet for Learnin**g

Use of ICT Equipment (including mobile devices) and the Internet must be appropriate to children’s education, staff professional development or the broader aims of the school.

* I understand that as an employee of the Trust there are Terms and Conditions that apply to my employment. Abuse or un- professional use of school equipment, or internet service if forbidden. Disciplinary action will be taken in line with Trust Policy.
* Access to social networking sites, chatrooms or user groups (other than for professional use agreed in advance with the Headteacher/ICT Leader) is forbidden.
* I understand it is my responsibly when using social networking sites to behave in a professional manner which reflects the values of our school. I understand that my responsibilities as an employee mean I should not condone inappropriate or illegal behaviours through my actions on Social Media.
* Access must only be made via the user’s authorised account and password, which should not be given to anyone else. Staff will be held responsible for access under their user ID.
* Do not download, use or upload any material which is unsuitable for use within the school or which compromises the security of the school network.
* Do not reveal or share any personal information or photographs about any member of the school, adult or child.
* Ensure that children using the Internet are supervised at all times.
* When using web sites in the classroom, always assess the web page before displaying to children.
* Email communications opened and sent during the school day should be relevant to your teaching role and responsibilities.
* I will use the ‘cloud space’ provided to store information that does not identify any children’s personal details.
* I will not plug in any personal USB storage devices as they could infect our network with malicious software.
* I will only use encrypted school issued devices to store information and all devices much be password protected.
* Material accessed via the Internet is not copyright free. Respect the copyright of information accessed via the Internet. Care must be exercised in using the web content and sources of material should be acknowledged.
* If unsuitable material is accessed inadvertently, the school’s IT Leader should be informed directly. Individual user’s Inter- net access will be monitored, including websites visited and e-mail use.
* If you see anything you are unhappy with or you receive messages you do not like, let the ICT Leader/Headteacher know immediately.
* The use of personal email accounts (on a school provided device) in school is permitted for occasional and unavoidable access, when children are not present. The use of a personal device when children are present is not permitted.
* I acknowledge that my use of the Internet in school will comply with the above guidelines and that a breach of the guideline may be investigated and subsequent disciplinary action could follow. Any variation to this agreement will be agreed with the Head Teacher or IT Leader in advance and in writing.
* Name:
* Signed Date:

**Appendix 9**

**Acceptable Internet Use Policy for Visitors**

**Remember that we use the computers and the Internet for Learnin**g

Use of ICT Equipment (including mobile devices) and the Internet must be appropriate to children’s education, staff professional development or the broader aims of the school.

* I understand that as an employee of the Trust there are Terms and Conditions that apply to my employment. Abuse or unprofessional use of school equipment, or internet service if forbidden. Disciplinary action will be taken in line with Trust Policy.
* Access to social networking sites, chatrooms or user groups (other than for professional use agreed in advance with the Headteacher/ICT Leader) is forbidden.
* I understand it is my responsibly when using social networking sites to behave in a professional manner which reflects the values of our school. I understand that my responsibilities as an employee mean I should not condone inappropriate or illegal behaviours through my actions on Social Media.
* Access must only be made via the user’s authorised account and password, which should not be given to anyone else. Staff will be held responsible for access under their user ID.
* Do not download, use or upload any material which is unsuitable for use within the school or which compromises the security of the school network.
* Do not reveal or share any personal information or photographs about any member of the school, adult or child.
* Ensure that children using the Internet are supervised at all times.
* When using web sites in the classroom, always assess the web page before displaying to children.
* Email communications opened and sent during the school day should be relevant to your teaching role and responsibilities.
* I will use the ‘cloud space’ provided to store information that does not identify any children’s personal details.
* I will not plug in any personal USB storage devices as they could infect our network with malicious software.
* I will only use encrypted school issued devices to store information and all devices much be password protected.
* Material accessed via the Internet is not copyright free. Respect the copyright of information accessed via the Internet. Care must be exercised in using the web content and sources of material should be acknowledged.
* If unsuitable material is accessed inadvertently, the school’s IT Leader should be informed directly. Individual user’s Internet access will be monitored, including websites visited and e-mail use.
* If you see anything you are unhappy with or you receive messages you do not like, let the ICT Leader/Headteacher know immediately.
* The use of personal email accounts (on a school provided device) in school is permitted for occasional and unavoidable access, when children are not present. The use of a personal device when children are present is not permitted.
* I acknowledge that my use of the Internet in school will comply with the above guidelines and that a breach of the guideline may be investigated and subsequent disciplinary action could follow. Any variation to this agreement will be agreed with the Head Teacher or IT Leader in advance and in writing.
* Name:
* Signed: Date :

**Appendix 10**



**Digital Image Consent – Pupil admission booklet**

Information regarding the use by the School and Media of digital content

Riverdale Primary School Data Protection Act 1998

Dear Parent/Guardian

As required by the Data Protection Act 1988, we are required to inform you of how we manage data relating to your child.

In Riverdale Primary School digital media is vital to record children’s learning journey and special events. Any image or recording is normally removed from the source within 72 hours and/or stored in a password/encrypted environment. These images are used for;

• Creating digital learning stories, using photos, videos and voice recordings.

• Sharing on Marvelous Me through a password protected system or sharing on other social media sites that are not protected.

• Group photos or images from events, visits and visitors attending school.

• Displays around school.

• Educational press releases (paper/electronic).

• Sharing on the Internet where children’s work is being used in an educational way to celebrate achievements. This includes the school and other websites plus School social media sites (i.e. Facebook and Twitter etc) to promote Schools achievements and keep parents and carers up to date with events/residentials. Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

• From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or for other high profile events. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes or other media.

Parents and carers may record events at School (eg Christmas Performance) of their own children but we ask you not to post these on social media that include other children without their parent’s consent. School cannot be held responsible for further sharing of these posts.

If you have any concerns regarding this consent then please email school on office@riverdaleprimary.org.uk. If no email is received in response to this letter, we will work on the basis we have your continued support and understanding of this policy.

Acceptance of School Policies, including Digital Media, use of the internet, safeguarding, Code of Conduct and others listed on our Website, and permission for local visits within the school day and for which no charge will be made.

Pupil \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature of Parent/Guardian\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_