RICHMOND HOUSE SCHOOL
Where children are happy to learn

E-SAFETY POLICY

At Richmond House School we will develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices as they develop their personalised learning, in line with our school's vision.

Network Manager: Bursar
E- Safety Co-ordinator – Kate Van Opstal
E- Safety Lead - Assistant Head, Pastoral - DSL

Introduction

It is the duty of Richmond House School to ensure that every pupil in its care is safe and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles;
- Smart Watches
- Mobile internet devices such as smart phones and tablets; and
- Home internet devices such as computers and Smart televisions.

This policy, supported by the Acceptable Use agreements (for staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies and documentation:

Data Protection Policy
Safeguarding and Child Protection Policy
Staff Code of Conduct
Health and Safety Policy
Behaviour Policy
Anti-Bullying Policy
Acceptable Use agreements
The PSHE and Computing Curriculum.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Richmond House School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes any person working in the school, but does not include supply staff from an agency or a volunteer; teaching and non-teaching staff, governors, and Visting Music teachers and regulated volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including supply teachers and occasional volunteers.

Both this policy and the Acceptable Use Agreements (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, smart watches etc.).

Roles and responsibilities

1. The Governing Body

The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness.

2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headteacher has delegated day-to-day responsibility to the e-safety co-coordinator and the Assistant Head who is the DSL.

In particular, the role of the Headteacher and the Senior Leadership team is to ensure that:

- staff, in particular the DSL and the e-safety co-ordinator, are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

3. The DSL and E- Safety Co-ordinator

The School's DSL is responsible to the Headteacher for the day to day issues relating to e-safety. The E-safety coordinator will work with the DSL and the school's network manager, the Bursar, and IT support team to ensure this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

4. Network Manager – The Bursar

The school's Network Manager is responsible for maintaining a safe technical infrastructure at the school. They will work with advice from our IT support team to keep abreast with the rapid succession of technical developments, to ensure the security of the school's hardware system and its data, and for training the school's teaching and administrative staff in the use of IT. The Network manager with support from the IT support team will maintain the filtering system and any inappropriate usage will be dealt with in line with the Disciplinary Procedure for staff or the Behaviour policy for pupils.

5. Teaching and support staff

All staff are required to read the school’s e-Safety policy and the staff code of conduct and sign the Staff Acceptable Use Agreement before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Staff must report any suspected misuse or problem to the E- Safety Co-ordinator or the DSL.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Agreement, and for letting staff know if they see IT systems being misused.

Parents of children in Year 1 and 2 are required to sign the pupil Acceptable Use agreement to acknowledge they have discussed this with their child. From Years 3-6, children and their parents will be expected to sign the Pupil Acceptable Use Agreement before being given access to school systems.

The Pupil Acceptable Use agreements are displayed in the computer rooms.

7. Parents and carers

Richmond House School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Pupil Acceptable Use Agreement.

Education and training

1. Staff: awareness and training

New staff receive information on Richmond House School's e-Safety and Acceptable Use Agreement as part of their induction.

All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. Any visitors using the school’s IT resources should read the e-safety policy and sign the Acceptable Use Agreement.

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 Acceptable Use Policy which must be signed and returned before use of technologies in school. 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.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

Any concerns regarding e-safety should be reported to the E- Safety Co-ordinator or the DSL. The DSL will keep a record of all e-safety incidents and concerns.

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out through PSHE lessons, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety (see Computing and PSHE curriculum documents for further details). Pupils can report concerns to the Safeguarding Lead, and any member of staff at the school.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Pupils should be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges information evenings for parents when advice is given about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

Publications and guidance for parents is uploaded on the Pastoral section of the School website.

Policy Statements

1. Use of school and personal devices in relation to the safety of others

Staff

School devices assigned to a member of staff as part of their role must have a password (which should be changed regularly) or device lock so that unauthorised people cannot access the content. When they are not using a device staff must ensure that it is locked to prevent unauthorised access.

Staff at Richmond House School are permitted to bring in personal devices for their own use. Staff are not allowed to use their personal devices while with children (except in emergencies while on the Sports Field or off-site) or at any time within the Early Years setting. They may use such devices only during break-times, lunchtimes, non-contact lessons or before/after the school day.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils and only with parents if unrelated to school business. Under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system for anything related to school business, unless in an emergency, with permission from the Head Teacher.

Pupils

Pupils must not bring mobile devices into school, unless they have been given permission by the Headteacher (e.g. for use during the journey to and from school). They must be handed in to the school office at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Headteacher or SENCO to agree how the school can appropriately support such use. The Headteacher will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites or any website or personal email which is unconnected with school work whilst in front of pupils. Such access may only be made during break-times, lunchtimes, non-contact lessons or before/after the school day and only on personal devices.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that all internet usage through the school network and staff email addresses is monitored.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the DSL or network manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Richmond House School into disrepute;
- breach confidentiality;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of any individual in the school.

Under no circumstances should school pupils be added as social network 'friends' or contacted through social media or personal email by any member of staff.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a parent / carer using any personal email address unless for school related business. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the Network Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff.

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the DSL or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the Bursar for assistance.

The PSHE curriculum includes advice on what is an appropriate and an inappropriate use of the internet.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy, Privacy Policy, Retention of Records Policy and the Acceptable Use Agreements for further details.

Pupils are expected to save all data relating to their work on the school network. Staff are expected to save all data relating to their work to their school laptop/ PC, to the school's central server or to OneDrive. Staff must not save work to the hard drives on these devices and take them from the building unless they are encrypted. Staff should be aware that information stored on the hard drive is not backed up and therefore could be lost in the event of a computer failure.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the network manager, the Bursar.

4. Password security

Pupils have storage folders on the server, which are used from Year 2 upwards.

Children in Reception do not have their own login to the school network. Pupils in Years 1 and 2 are given an individual passwords by their teacher. Pupils in Years 3 upwards must change their password, a copy of which is kept for staff use in the computer rooms.

Members of staff will keep children's passwords in a secure place. Otherwise, pupils and staff must not write down passwords or share them with others.

Staff should ensure they use strong, unique passwords (usually containing eight letters or more, and containing upper and lower case letters as well as numbers), which should be changed if there is any risk to security.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims on school equipment, but must follow school policies regarding the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

School adheres to the following checklist when publishing images of pupils:

- ensure students are dressed appropriately. At sports events for example, we will not publish pictures of pupils in swimming costumes.
- ensure electronic images are stored confidentially and securely and are accessed only by staff with authority to do so
- never show, copy, or give an image to any unauthorised person
- avoid using the last name of a pupil and will always ensure that parents have consented to use of images before publishing the image

Pupils must not take, use, share, publish or distribute images of others.

School handles the images according to its obligations under the Data Protection Act 2018.

6. Misuse

Richmond House School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures in particular the Safeguarding Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in the school in line with our Anti-Bullying and Behaviour policies.

Complaints

As with all issues of safety at Richmond House School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the Assistant Head, who is the DSL, in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate.

Incidents of or concerns around e-safety must be reported to the school's Designated Safeguarding Lead, in accordance with the school's Child Protection Policy.

Date last reviewed by the Governing Body: October 2019

A review of this policy, through the Governonig Body and the SLT, is undertaken within 3 years of the last review date.

Helen Stiles

Signed Head teacher

Signed Chair of Governors

Appendix 1

Pupil Acceptable Use Agreement for Upper School Pupils
Richmond House School

Richmond House School uses a wide variety of tools to enhance teaching and learning, including technology and the internet. The use of technology can broaden the kind of tasks undertaken, can enrich lessons, provide opportunities for differentiation and enable work to be completed more effectively. The school takes all reasonable steps to ensure safe internet access at all times, but pupils must also understand how to use the internet responsibly and safely. Antisocial and potentially harmful behaviour of any kind through the misuse of technology in unacceptable and will be dealt with according to the School's behaviour policy. This applies to activity offsite as well as at school if it has a negative impact on members of the school community.

It is important that pupils read and understand the following rules and expectations. We would like all parents/guardians to discuss the following rules with their children and sign below.
I will keep myself safe by

- Keeping my passwords secure and not sharing them with others
- Not sharing any personal information about myself when on-line
- Telling an adult if I see anything unpleasant or inappropriate, or anything that makes me feel uncomfortable when I see it online

I will treat others and the school with respect by

- Looking after all school computers and other equipment.
- Not installing any programs on school computers.
- Not using the internet to cause distress or to bully others.
- Not posting pictures, videos or anything else onto the internet, unless a teacher is with me.
- Not accessing social networking sites (such as Facebook) during school time.
- Not bringing in a mobile phone or other devices that can be connected to the internet unless with permission from Mrs Stiles. If permission is given, the phone must be handed in to the office during school time.
- Telling an adult if I know someone else isn't using technology in the right way.
- Not using others' passwords , interfere with others accounts or log in as someone else
- Not encouraging or putting pressure on others to act in a way which threatens their online safety on the online safety of another pupil
- Not using internet to look at anything that is illegal, inappropriate or abusive.

When using the internet for research I am aware that I

- Must not use the original work of others and say it is my own work
- Must not download pictures or information if work is protected by copyright
- Must take care to check information is from a reliable and accurate source

I am aware that the school will check my use of school technology and the internet.

I agree to follow the above rules whenever I use Richmond House School's technology or my own technology in a way that relates me being a member of Richmond House School.

Name of Pupil ____

Signed: _____________________________ (Pupil)   Date: ______________

Signed: _____________________________ (Parent)   Date: ______________

Appendix 2

Pupil Acceptable Use Agreement for Lower School Pupils
Richmond House School

Richmond House School uses a wide variety of tools to enhance teaching and learning, including technology and the internet. The use of technology can broaden the kind of tasks undertaken, can enrich lessons, provide opportunities for differentiation and enable work to be completed more effectively. The school takes all reasonable steps to ensure safe internet access at all times, but pupils must also understand how to use the internet responsibly and safely. Antisocial and potentially harmful behaviour of any kind through the misuse of technology in unacceptable and will be dealt with according to the School's behaviour policy. This applies to activity offsite as well as at school if it has a negative impact on members of the school community.

It is important that pupils read and understand the following rules and expectations. We would like all parents/guardians to discuss the following rules with their children and sign below.

- I will look after all school computers and other equipment.
- I will follow all instructions when using technology in school.
- I will not use the schools' technology to cause any upset or harm to others.
- I will tell a teacher if I know someone else is not using technology in the right way.
- I will keep my passwords private and will not use other students' passwords.
- I will not use the internet to look at anything that I have not been told to look at by a teacher.
- I am aware that the school will check my use of school technology and the internet.

I have read and discussed the school e-safety rules with my child.

Signed: ___________________________________ (Parent)   Date: ______________

Appendix 3

STAFF AND ANYONE GIVEN ACCESS TO THE SCHOOL NETWORK

ACCEPTABLE USE AGREEMENT

I confirm that I have read and understood the e-safety policy and the staff code of conduct and I will use all means of electronic equipment provided by the school and any personal devices which I use for school activity in accordance with this policy and the staff code of conduct.

Terms of Agreement

I understand that I must use school systems in a responsible way to ensure that there is no risk to my professional or personal online safety or the online safety and security of the systems and other users.

- Any online communications or any communications sent from a school email address will be professional and respectful of others and maintain the reputation of the school.
- To protect my own privacy, I will only use a school email address and school phone numbers (including school mobile phones) as contact details for children and their parents, unless in a case of emergency.
- I will not share any personal telephone numbers, email accounts or social media accounts with pupils.
- I will not communicate with parents using personal phone numbers, email accounts or social media accounts on matters of school business.
- I shall only communicate with parents about matters relevant to School life using official School systems: all such communications will be professional in tone and manner
- To protect the privacy of others I will only store confidential child information, personal child information or data on a device that is encrypted or protected with a strong password. I will ensure that school computers are fully logged off or the screen is locked before being left unattended.
- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.
- I will not use my personal mobile phone or other personal electronic equipment to take photographs or videos of children.
- I will only use school equipment to take any photographs or videos of children, with their consent
- I will not use my personal mobile phone or access social media accounts or any website or personal email when with the children.
- I will follow the staff Code of Conduct in regards to school technology
- Any remote work I do away from the school building will be password protected
- I undernstand that any personal mobile devices are filtered when used through the school network

- I will treat all equipment belonging to the school with respect and care.
- I understand that the School’s digital technology systems are primarily intended for educational use and that I shall only use the systems for personal or recreational use within the rules set out in the School’s Staff Code of Conduct

I understand that the school may monitor or check my use of school based ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the School’s disciplinary procedures.

Name …………………………………………………………………..

Signed ……………………………………………………………….

Date …………………………………………………………………

Appendix 4

Volunteer or Visitor with access to the Network Acceptable Use Agreement

Richmond House School

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all visitors are aware of their responsibilities when using any form of ICT. All volunteers and visiting professionals who have access to the school network are required to read and sign this agreement and will specifically adhere to the following points in relation to their own conduct.

- I understand that school ICT equipment, including computers, laptops, digital cameras, mobile phones and any other form of communication technology, is provided by the school for the purposes of teaching and learning, and/or ensuring pupils' safety.
- I understand that I am not permitted to use my personal mobile phone or handheld ICT device during working hours while teaching or supervising pupils, unless in exceptional circumstances.
- I will not install any software or hardware on school ICT equipment without permission.
- I will ensure that all personal data (such as data held on SIMS) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Head.
- I understand that my use of school information systems, including the internet and email, can be monitored and logged and can be made available, on request, to the Head teacher.
- I understand that my own personal digital or mobile cameras are expressly forbidden to be used in school.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will respect copyright and intellectual property rights.
- I will comply with the ICT system security and not disclose any passwords provided to my school. I understand that I am responsible for all activity carried out under my user name.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any incidents of concern regarding children's safety to the e-safety Coordinator, the Child Protection Officer or Head Teacher.

Signed: ________________________________ Print name: ______________________

Purpose of visit: ___________________________________ Date: ______________

APPENDIX 5 Use of Mobile Phones and Cameras for EYFS

Richmond House School EYFS allows staff to bring in personal mobile telephones and devices for their own use.
Staff bringing personal devices into Nursery and Reception must ensure there is no inappropriate or illegal content on the device.
All staff must ensure that their mobile phones/devices are locked away throughout contact time with children.
Mobile phone calls may only be taken at staff breaks or in staff members' own time. If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile either outside or in the Staff Room (where no children are present).
If any member of staff has a family emergency or similar and are required to keep their mobile phone to hand, prior permission must be sought from the Head teacher.

Cameras

Photographs are taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements. It is an effective form of recording their progression in EYFS.
They may also be used on our website and/or by the local press with permission from the parents. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.
Only the designated Nursery and Reception cameras and iPads are to be used to take any photos within school or on outings. Images taken on this camera must be deemed suitable without putting the children in any compromising positions that could cause embarrassment or distress.
All staff are responsible for the location of the camera and iPads; these should be put away securely at the end of the day. Images taken and stored on the camera must be downloaded as soon as possible, ideally once a week. Images must only be downloaded by EYFS members of staff.
Under no circumstances must cameras of any kind be taken into the washrooms. If photographs need to be taken in a bathroom, i.e. photographs of the children washing their hands, then the EYFS Co-coordinator must be asked first and staff be supervised whilst carrying out this kind of activity.
Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.
This document should be read in conjunction with the Safeguarding and Child Protection Policy and the Staff Code of Conduct.