

Online Safety Policy

Introduction

King's Infant School provides a safe environment for all its pupils and staff. It applies the same principles to the 'virtual' or digital world as it applies to the school's physical buildings by providing clear advice and guidance on how to minimize risk and how to deal with any infringements. Staff and pupils are involved inside and outside school in a whole range of emerging technologies such as smartphones, blogging and gaming sites and it is our duty to protect them.

Objectives

By providing clear advice and guidance, KIS aims to:

- Enable pupils and staff to make safe choices when using the technologies used above
- Protect pupils and staff from misuse of technology
- Have clear procedures in place to deal with any infringement

Organisation and Planning

KIS recognizes that e-Safety is an essential aspect of strategic leadership within this school and the Headteacher, with the support of the Senior Leaders and King's Group, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored.

The School Computing and E-Learning Coordinator keep up to date with Online Safety issues and guidance and ensures the Headteacher, Senior Leadership and King's Group are updated as necessary.

The Board have an overview understanding of Online Safety issues and strategies at KIS. The Board are aware of the guidelines on Online Safety and are updated at least once annually on policy developments.

The IT Team support the Computing and E-Learning coordinator in the development and implementation of appropriate Online Safety procedures. They ensure there is a technical infrastructure to support safe practices while ensuring that learning opportunities are maximized.

All teachers are responsible for promoting and supporting safe behaviours in the classrooms and following school Online Safety procedures. Central to this is fostering a "No Blame" culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Annually, all KIS staff are made aware of the school's expectations with regard to:

- the safe use of email
- the safe use of internet including the use of internet based communication services
- the safe use of school network, equipment and data
- the safe use of digital images and digital technology
- cyberbullying procedures
- their role in providing safety education for pupils

Whenever a pupil or a staff member infringes the Online Safety Policy, the incident is recorded in the Online Safety Incident Log which is kept jointly by the E-Learning Coordinator and the Designated Safeguarding Leader. The final decision on the level of sanction will be in accordance with approved school policies and Spanish Law. Staff members must complete the incident log and deal with Online Safety issues.

If a member of staff commits an exceptionally serious act of gross misconduct, such as use or storage of child pornography they will be immediately suspended. An investigation will be held before any disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Child Pornography

In the case of Child Pornography being found, the member of staff will be immediately suspended.

How will staff and pupils be informed of these procedures?

- All staff will be required to sign the school's Online Safety Acceptable Use Policy Agreement (AUPA)
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'
- The school's Online Safety Policy will be made available and explained to parents, and the iPad rules (see appendix)
- Information on reporting cyber bullying will be made available by the school for pupils, staff and parents

Online safety complaints procedures

KIS will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by teacher/e-Learning Coordinator/Headteacher
- informing parents or carers
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system
- suspension

Our Computing and E-Learning Coordinators act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyber bullying are dealt with in accordance with our Behaviour Policy and Safety Guidance. Complaints related to safeguarding are dealt with in accordance with school safeguarding procedures.

In extreme cases the school reserves the right to search pupils for 'banned items' and 'delete data' stored data on a seized device. Items banned under the school rules are determined by the Headteacher and publicised in the school's behaviour policy (see Electronic Devices- Searching and Deleting, Appendix 3).

All issues are recorded in the Online Safety Incident Log (Appendix 2).

Managing email safety

Email is now an essential means of communication for staff and pupils at King's Infant School and at home. Directed email use brings significant educational benefits through increased ease of communication between pupils and staff, or within local and international school projects. KIS reserves the right to monitor email to provide a safer email environment for pupils.

Pupils are made aware of the risks and issues associated with communicating through email and the strategies to deal with inappropriate emails as part of the school's Online Safety and anti-bullying education programme.

Pupils are taught about the safety and 'netiquette' of using email i.e.



- not to give out their email address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer
- that an email is a form of publishing where the message should be clear, short and concise
- that any email sent to an external organisation should be written carefully and authorised before sending
- they must not reveal private details of themselves or others in email, such as address, telephone number, etc
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- embedding adverts is not allowed
- that they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature
- not to respond to malicious or threatening messages and emails but to keep and report them as evidence
- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them
- that forwarding 'chain' email letters is not permitted

Managing the internet safely

KIS supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access. Staff preview all sites before use.

The curriculum context for Internet use is planned to match pupils' ability, using pupil friendly search engines where more open Internet searching is required. All users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse –through staff meetings and teaching programme. KIS keeps a record of any bullying or inappropriate behaviour.

KIS fosters a 'No Blame' environment that encourages pupils to tell a teacher/adult immediately if they encounter any material that makes them feel uncomfortable.

KIS has a clear, progressive Online Safety education programme throughout all Key Stages, built on UK national guidance.

When copying materials from the web, KIS ensures that staff and pupils understand issues around plagiarism, how to check copyright and also know that they must observe and respect copyright/intellectual property rights;

Training is provided to staff on the Online Safety education programme and the school runs a rolling programme of advice, guidance and training for parents, including demonstrations, practical sessions held at school and suggestions for safe Internet use at home.

Managing digital images and video safely

The KIS website is an important, public facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it is an effective way to share the school's good practice and promote its work.

A senior member of staff oversees and authorises the website's content and checks suitability. When uploading digital images or video KIS follows the following practice:

- Pupils are not fully named instead the first name and capital letter of surname are used eg Luis C.
- If showcasing examples of pupil's work use only first names
- Parental permission is obtained upon admission to KIS for publishing any photographs or video footage of pupils on the school website or in a DVD.
- Links to any external websites are thoroughly checked before inclusion on the website and newsletters to ensure that the content is appropriate both to the school and for the intended audience.

Using the school network, equipment and data safely

The computer system and network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet or email activity on the network.

Monitoring and review

Computing and E-Learning Coordinator in each School provide strategic leadership in the teaching of Online Safety. Together with the Headteacher, they are responsible for the quality of teaching and for monitoring the standard of pupils' work. By keeping abreast of best practice, they support the professional development of class teachers in this area.

Computing and E-Learning Coordinator meet class teachers regularly to review individual examples of work against the National Curriculum.

The Online Safety Committee have a twice annual meeting to review school policy, look at incidents and report on the strengths and weaknesses of the School's performance in this area and indicate areas for improvement (see Online Safety Committee Appendix 1).

KIS has the following documents available within the school:

- KIS Online Safety Guidelines
- Digital Images and Video Safety Guidelines
- Using the school network, equipment and data safety Guidelines

Key Responsibilities

- E-Safety Rules
- Acceptable Use Agreements
- Online Safety Incident Log
- Infringement and Sanction Guidelines

Created and Reviewed by: Dawn Akyurek, September 2016 Kirsty Sharp, October 2016	Policy Category: Health and Safety
Approved by: <i>King's Group Board</i>	Date: October 2016
	Next Review: August 2017

Appendix 1 Online Safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The online safety committee will seek to include representation from all stakeholders.

The composition of the group should include

- SLT member/s
- Designated Safeguarding Leader
- Computing and E-Learning Coordinator
- ICT Technical Support staff (where possible)

At least one member of the committee must be a member of the teaching staff.

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary and the minutes of the meeting

will be sent to a Governor.

- 2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
- 2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
- 2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held twice a year. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the Computing and E-Learning Coordinators with the following:

- To keep up to date with new developments in the area of online safety
- To review and develop the Online Safety Policy in line with new technologies and incidents
- To monitor the delivery and impact of the Online Safety Policy
- To monitor the log of reported online safety incidents and to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through: staff meetings, pupil forums and surveys, governors meetings, parents evenings, website/VLE/Newsletters, internet Safety Day



King's Infant School
The British School of Madrid

Chamartin

- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyber bullying for staff and pupils

6. AMENDMENTS

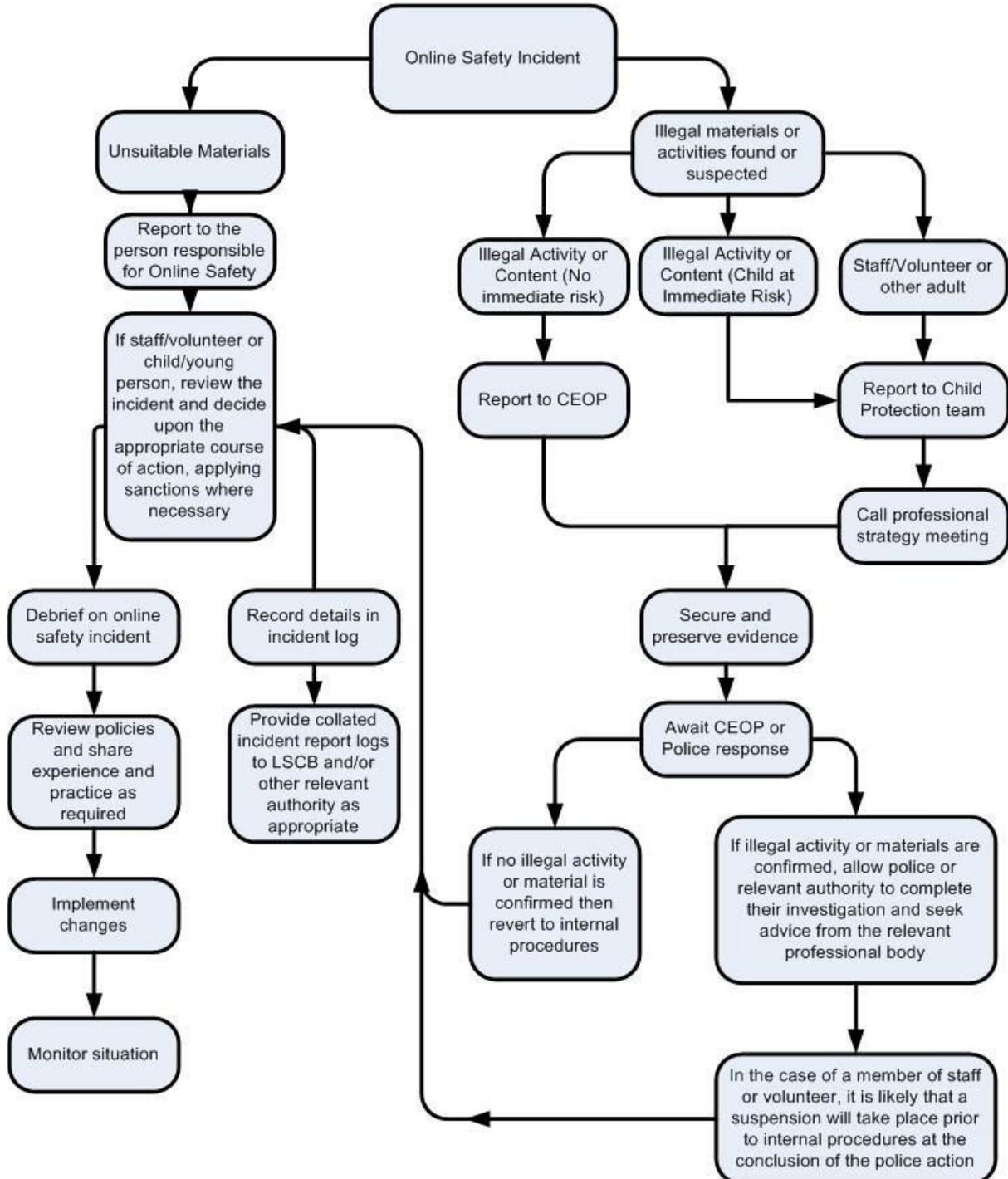
The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for King's Infant School, Chamartin have been agreed



Appendix 2

Responding to incidents of misuse – flow chart



Appendix 3

Electronic Devices - Searching & Deletion Policy

Introduction

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. One particular change is the power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

The items banned under school rules are as follows:

- mobile phones
- personal computers and laptops
- tablets

These items can be searched for by an authorised member of staff with or without the permission of the pupil.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation.

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

- Designated Safeguarding Leaders/SLT

Training / Awareness

All members of staff are aware of the school's policy on "Electronic devices – searching and deletion". The members of staff that are authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices have received training that is specific and relevant to this role.

Only members of staff with a Level 3 safeguarding certificate will be able to judge whether material that is accessed is inappropriate or illegal and therefore can be deleted.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils are allowed to bring mobile phones or other personal electronic devices to school but these must be deposited at reception upon entering the school.

If pupils breach these rules then they will be sanctioned according to the rules outlined in the behaviour policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the *pupil* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *pupil* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:

The person conducting the search may not require the *pupil* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

‘Possessions’ means any goods over which the *pupil* has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the *pupil* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so. The examination of the data / files on the device will go only as far as is reasonably necessary to establish the facts of the incident.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material (if it poses a risk to the physical or mental harm of a child), retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. *A record will be kept of the reasons for the deletion of data / files*

Care of Confiscated Devices

School staff are reminded of the need to ensure the safekeeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

Audit / Monitoring / Reporting / Review

The responsible person Headteacher will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files using the Online Safety Incident Log.

These records will be reviewed by the Online Safety Committee at regular intervals.

This policy will be reviewed by the Headteacher and governors annually and in response to changes in guidance and evidence gained from the records.

DfE guidance can be found at:
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>



Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology in a secure and safe environment. For my professional and personal safety:

- I understand *that the school* will monitor my use of the school digital technology and communications systems.
- I understand that the school digital technology systems are primarily intended for educational.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital video/images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school when appropriate.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and King's Group has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date antivirus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed



necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and in situations related to my employment by the school .
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

Rules for using the iPads in School. These rules are taught to the children during computing and PSHE lessons, These rules are also shared with the parents. So they can use similar rules in the home to keep the children safe in their computer/ tablet/ iPad use.



King's Infant School
The British School of Madrid

Chamartin