ALPHA PREPARATORY SCHOOL
E-SAFETY POLICY

This policy relates to the whole school, including the Early Years Foundation Stage (EYFS).

WHAT IS E-SAFETY?

E- safety is defined as being safe from risks to personal safety and well-being when using all fixed and mobile devices that allow access to the internet as well as those that are used to communicate electronically. This includes, but is not limited to, computers, laptops, cameras, music devices, mobile phones, tablets and gaming consoles. These devices are referred to in this policy as information and communication technologies (ICT).

Alpha Preparatory School recognises that these are valuable tools that can be used to promote pupil learning and achievement; provide pupils with essential skills for 21st century life; support the professional work of staff and enhance the administration and management of the school.

The use of communications technology and the internet brings many benefits to everyone in the school community, but it is important that these technologies are used responsibly, safely and appropriately. All members of the school community should be aware of their responsibilities, how to practice good e-safety and what they should do if they have concerns or feel at risk.

WHAT ARE SOME OF THE DANGERS?

Unfortunately, some adults or young people may use these technologies to harm children. Examples include sending hurtful or abusive texts; enticing children to engage in sexual conversations, webcam filming, photography or face-to-face meetings; use of social media to bully or otherwise cause harm.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed in line with our Anti-Bullying Policy.

Websites, particularly those with a social media aspect, can also be used to radicalise and draw young people into supporting extremist ideologies.

Additionally, poor practice can result in school data becoming compromised.

POLICY AIMS

This policy provides the platform for regulating digital activity in school and for educating all members of the school community on the dangers inherent in the use of these technologies and how to manage them. It outlines responsibilities and expected conduct. It will aid our

intention to educate pupils about the benefits and risks of technology, giving them the skills to evaluate online information and to take care of their own safety and security.

ROLES AND RESPONSIBILITIES

The School E-safety coordinator is Mr D Gonsalves (Director of STEM Innovation) and the nominated E-safety governor is Mr K Shah. Mr Gonsalves is also our computing curriculum coordinator. In addition, all members of the school community have a responsibility to use information and communications technologies (ICT) in an ethical and responsible manner and Acceptable Use agreements can be found at the end of this policy and also within the school's Code of Conduct.

COMMUNICATING SCHOOL POLICY

This policy is available on the school website. E-safety posters and guidelines are displayed around the school. E-safety is integrated into the curriculum in any circumstances where the internet or technology are being used, and is explicitly addressed in computing lessons and PSHEE discussions. The school also has a team of pupil Digital Leaders, who work with our E-Safety coordinator to raise awareness of E-Safety issues amongst the pupil body.

SECURITY OF THE SCHOOL'S COMPUTER NETWORK

Internet access is provided through the London Grid for Learning (LGfL), who provide a firewall and content filtering to ensure that access is appropriate to the age and maturity of our users. Anti-virus software is also installed and kept up-to-date. The school network is protected, as far as is practicably possible, against viruses, hackers and other external security threats. We recognise that no system is without vulnerabilities and our systems are regularly checked and maintained by our IT support technicians, working in tandem with the E-safety coordinator/Computing coordinator.

If staff or pupils discover unsuitable sites, then the URL should be recorded by the staff member or pupil (if old enough) and reported to the school E-safety coordinator/computing coordinator. This will be reviewed and appropriate action taken. For example, a website or URL may be blocked from anyone accessing it again. Any material found by members of the school community that is believed to be unlawful will also be reported to the appropriate agencies.

The school also uses Smoothwall eSafe to provide intelligent end-point monitoring by trained staff. Their reports give early warning of incidents and potential threats and allows the school to take appropriate and timely action. All monitoring data is processed in accordance with our Privacy Statement, which can be found on the school website.

Some additional safeguards that the school takes to secure our computer systems are:

- Enforcing the use of user logins and passwords to access the school network
- Separation of the curriculum and administration network and differing levels of user access
- Making sure that unapproved software is not downloaded or installed onto school computers. Requests for installation of programs must be made to the computing coordinators, who will check that the program is legitimate, safe and appropriate.

- No unauthorised media will be used on the school's network.
- Portable media containing school data will not be taken off-site without specific permission from a member of the senior management team. Only secure media (encrypted/password protected) approved by the school will be used for this purpose.

EMAIL

The school staff email account provided through LGfL should be used for all school-related business. It should not be used for personal purposes, nor should personal email accounts be used for school business. This separation between work and personal accounts is important for confidentiality. The school reserves the right to monitor school emails and their contents if it feels there is reason to do so.

Staff should be aware of the following when using email in school:

- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Email communication with parents or carers will generally be directed through the office. If there is a need for a direct communication, staff should seek approval from a member of the senior management team.
- Staff must check their school email regularly and at least once a day to ensure that school business is attended to in a timely manner.
- Staff must inform a member of the senior management team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They must not attempt to deal with this themselves.
- The forwarding of chain letters is not permitted.
- Staff should not open attachments or click on links contained in emails from unsolicited or unverified sources.

THE SCHOOL WEBSITE

The school website is a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for keeping parents, staff and pupils up-to-date with school news and events, celebrating achievements and promoting school projects.

Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy. The point of contact on the website will be the school address, school email and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils will be selected carefully. Pupils' full names will not be used on the website or associated with images without the consent of parents. The Headmaster, Mr P Fahy, is responsible for maintaining the content on the school website and ensure that these safeguards are not breached. Some departments have created blogs, such as science/STEM, music and French. It is the responsibility of the Heads of Departments of individual subjects to maintain the content of the blog and ensure safeguards are not breached.

SAFE USE OF DIGITAL AND VIDEO IMAGES

Photographs and examples of pupils' work bring our school to life, showcase our students' talents and add interest to publications and displays. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the GDPR and Data Protection Act 2018, images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school, parents/carers will be asked to sign an image consent form. The school does this to prevent repeatedly asking parents, which is time-consuming for both parents and the school. The terms of use of images never change, and so giving consent to the use of images over a period of time rather than a one-off incident does not affect what parents are consenting to. Parents may withdraw their consent at any time.

The school will put the following safeguards into place:

- Ensure parental consent is obtained. Consent will cover the use of images in: a) all school publications b) the school website c) newspapers as allowed by the school d) videos made or photographs taken by the school or in class for school projects.
- Staff will use school equipment, where possible, for recording images. In order to 'capture a moment' there and then, staff members can use their personal devices with the consent of the Headmaster. Any images or recordings taken of children must be uploaded to the school network if necessary, and then deleted from the staff member's device.
- Names of photographic files uploaded will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse, for example by ensuring that pupils are appropriately dressed.
- For public documents, including newspapers, full names will not be published alongside images of the child.
- Making parents aware that events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Any photographers that are commissioned by the school will be appropriately checked, will wear identification at all times and will not have unsupervised access to the pupils.
- Images taken on school devices, and personal devices (if consent has been provided), should be downloaded into the appropriate network folder as soon as possible and then deleted from the school device.

Please refer to our school policy on Safeguarding and Child Protection for more information on safeguarding in school and to the Privacy Notices available on the school website.

SOCIAL NETWORKING, SOCIAL MEDIA SITES and GAMING

Children are not allowed to access social media sites in school, unless these are moderated and part of the school curriculum, such as the school blogs. However, they are educated on the dangers of other sites and how to use them in safe and productive ways. Social media apps are extremely popular and we encourage parents to speak openly to their children about the apps their children may have uploaded. It is a parent's responsibility to check that their child is age-appropriate, with an appropriate ability, to have access to the sites and apps their child visits or uploads: a vast majority of apps and social media outlets have an age limit of

13-years-old, which children in a primary school setting should not be accessing. It is also a parent's responsibility to address any incidents which occur on social media outside school. Should a parent consent to their child's use of social media platforms, including WhatsApp, the parent is also consenting to deal with any repercussions of any interaction their child may experience. The school will not get involved in disputes between parents and/or children related to social media accessed outside school. Should a parent wish to inform the school of any online incidents outside of school, particularly if they feel there is a concern of safeguarding, they should contact the school office and they will be directed to the relevant member of staff. We also encourage the children, through PSHE, circle time and assemblies, to speak up as soon as possible if they feel uncomfortable with anything they see or have been sent online.

Staff should not refer to matters of school business when using personal social media and appropriate and professional online behaviour is expected at all times. Staff will not invite, accept or engage in communications with pupils in any personal social media. Any such communications received from pupils must be reported to the Designated Senior Person for Child Protection (see Safeguarding and Child Protection Policy for details). Staff should also not accept any social media communications from any ex-pupils under the age of 18. Staff are strongly advised to set all privacy levels to the highest settings on any personal social media accounts. Parents are also expected to respect privacy and to avoid postings which undermine good working relationships within the school community.

Pupils are only allowed to access educational games online when using the school network.

MOBILE PHONES AND PERSONAL DEVICES

Mobile phones and other personal communication devices (for example, devices which can access the internet, record/transmit text, sound or images) are common place in today's society and have many legitimate uses. However, within a school context there are particular issues which must be addressed. Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyber bullying.
- they can be used to access inappropriate internet material.
- they can be a distraction in the classroom.
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.
- they are valuable items which could be stolen, damaged or lost.

The school will put the following safeguards into place:

Pupils:

- Pupils are not allowed to bring mobile phones or other personal communication devices to school.

Staff:

- Staff mobile phones (or other devices) must not be used during lessons or while supervising pupils, except in emergency circumstances. In general, mobile phones

should not be used in the presence of pupils, unless necessary for safeguarding purposes.

- In order to 'capture a moment' there and then, staff members can use their personal devices with the consent of the Headmaster. Any images or recordings taken of children must be uploaded to the school network if necessary, and then deleted from the staff member's device.
- Staff should not communicate with pupils using any personal devices, including mobile phones, and any inappropriate communications received by staff from pupils must be reported to the Designated Safeguarding Lead (see Safeguarding and Child Protection policy for details). This also relates to our messaging service on Show My Homework.

CYBER BULLYING

Cyber bullying is the use of electronic devices to bully a person, for example by sending threatening or abusive text messages and malicious postings using social media. Cyber bullying, as with any other form of bullying, is taken very seriously and will be dealt with in accordance with our anti-bullying policy. In serious cases, a response under our Child Protection procedures may be warranted.

PROTECTING PERSONAL DATA

The school collects personal data from pupils, parents and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress and strengthen our pastoral provision.

We will ensure that any data we collect and process is used correctly and only as is necessary. National curriculum results, attendance and registration records, special educational needs data and any relevant medical information are examples of the type of data that the school needs.

In line with the GDPR and Data Protection Act 2018, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that processed data is accurate
- not keep data longer than is necessary
- ensure that data is secure

There may be circumstances where the school is required by law or in the best interests of our pupils/staff to pass information onto external authorities, for example – the local authority and the Department for Education. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Further details can be found in our Data Protection Policy and in our Privacy Notices.

COMPLAINTS REGARDING E-SAFETY

Complaints about breaches of E-safety will be dealt with by the Headmaster, with advice from the E-safety coordinator as necessary. The Headmaster may delegate a member of the team to respond to any parental concerns raised with regards to E-safety. See the school's safeguarding and child protection policy for further details.

E-safety incidents will be recorded in an E-safety incident log by the Headmaster/E-safety coordinator. The regular review of the incident log and the actions taken will be part of the review of how effectively this policy is implemented (see section below).

MONITORING AND REVIEW

Technology is progressing rapidly and new technologies will inevitably continue to emerge. The school will assess the risks and educational benefits of any new technologies before they are allowed into school. This policy will be reviewed annually or when the need arises by the Computing/E-safety Coordinator, the Headmaster and the nominated governor. A statement of the review and any recommendations will be presented to the Governing Body for further discussion and endorsement.

ONLINE ZOOM SESSIONS

All parents, children and staff are issued the following guidance before formal remote lessons commence…these were first issued in April 2020 at the start of the pandemic:

ALPHA PREPARATORY SCHOOL
Our Zoom Sessions – Pupil Guidelines

We ask parents to go through these guidelines for using Zoom with your children.

1. Be Prepared

Always be ready for your Zoom session. Before the session, you should make sure you have all the equipment you need - pencils, pens, erasers, rulers, worksheets etc. Always remember to have paper or a book to write in. Make sure you have a drink available before the session starts.

2. Stay in One Spot during the Zoom Lesson

It is distracting to your teacher and the rest of your class if you move around. If you wish to go to the lavatory, you do not need to ask the teacher for permission – if you do need to go, try not to miss any instructions as these will not be repeated.

3. Use a Clear Background

Zoom has lots of fun backgrounds, but it makes it very difficult for your teacher to see you. Keep fun backgrounds for your friends and family. If possible, find a spot in your house that has a simple, plain background and has good lighting. Try not to sit directly in front of a window with the light streaming in behind you; that will also make it hard for people to see you.

4. Find a Good Spot for Your Sessions

To avoid distractions, find a quiet spot in your house. It will be easier for you to hear your teacher, but ensure an adult is nearby in case you need them.

5. Be On Time

When you log in you will wait in a virtual waiting room until your teacher logs you into the virtual lesson. Your teacher will wait until everyone is there so try not to keep the class waiting by being late.

6. Wait Your Turn

Your teacher will give you a signal to use, like raising your hand, if you have something to say. Use good manners by using this signal, the same as if you were in class, before speaking. The teacher may request you to use the mute button or they may mute all students in the session.

7. Be Presentable

Take a few minutes before the session to make yourself as presentable as possible.

8. Be Respectful

During your Zoom sessions with staff and classmates, you should try to behave like you would in your class at school. You would not eat snacks or talk with your family members during a class at school, so please try not to do it during the online session.

Don't make fun of or say unkind things about anyone. You would not do this at school, the same rules apply during an Alpha Zoom session.

9. Listen carefully

Make sure you listen carefully to the instructions, Zoom sessions are very different from a lesson in the classroom and at first it may be harder to concentrate. If you do not understand, or would like something repeated, use the given signal to ask for help or for the teacher to repeat any instructions. Remember, if you leave the visibility of the screen, the teacher will not repeat their instructions.

ALPHA PREPARATORY SCHOOL
Our Zoom Sessions – Parent Guidelines

Zoom is one of the most popular video conferencing applications at the moment and it is now being used widely in schools to support teaching during the COVID-19 lockdown.

Zoom can monitor a pupil's activity, allowing a member of staff to track real-time activities, screen-share, record live lessons and recall video, audio, transcript and chat files. This resource is a great way to attempt to replicate classroom learning, however, as with all platforms there have recently been concerns over security but the school will take measures to maximise the use and security whilst utilising Zoom.

Alpha Preparatory School will be using Zoom sessions to complement their online learning platform and every care will be taken to ensure children's safety when engaging in an online lesson or online activity with a member of staff.

Below is a guide setting out how Zoom will be used as securely as possible and how you can do the same at home:

- Alpha Preparatory School will ensure the latest version of Zoom is available and this will be updated when any new upgrades become available. These updates will ensure the platform will not be vulnerable to hacking and will maximise security.

- All Zoom lessons will be set up by the Host (i.e. Alpha Preparatory School) using a meeting ID number and entry to the session will be password protected, only allowing those invited to each session to sign in. This is intended to stop the possibility of sessions being hacked by external sources. The password and link will be sent to invitees via an official school email, ending in @alpha.harrow.sch.uk so only those intended to join can access the virtual classroom.

- The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the Host to screen them before entering. This feature will be enabled and pupils will be admitted to the session by the Host. This function adds another layer of security to reduce the likelihood of 'Zoom Bombing'. (unauthorised people joining meetings uninvited and broadcasting inappropriate material).

- Once the lesson has started, the Host will 'lock the classroom' meaning no one else can join the session again, protecting the virtual classroom from anyone entering who is not welcome.

- Privacy controls will be set so that screen sharing is limited to the Host only. This reduces the risk of hacking or the installation of malware.

- Whilst the online sessions are taking place, we ask parents not to record the sessions on their devices. Any work delivered, set or provided during these online sessions and on our online learning platform, should not be shared with any one other than children on the Alpha register and their parents.

- During the online sessions, we ask parents not to interact with the member of staff. The Host is there for the children and not to interact with the parents.

- Pupils will be reminded that, despite being at home, the same level of behaviour and conduct exists as if they were at school i.e. to listen to instructions, be polite and remember their manners.

- Pupils will be reminded that inappropriate behaviour will result in them being removed from the session.

- The Host will be focused on teaching the children, interacting with them and supporting them. Should a child wish to visit the lavatory or leave the visibility of the screen during a session, this will not be addressed by the member of staff.

- Computers should be positioned in an open environment within the home, where possible, in order for the pupil's activity to be monitored by an adult in the house if necessary.

- In order to enhance the learning experience, the background used in Zoom should be as neutral as possible, with good quality lighting and sound.

ALPHA PREPARATORY SCHOOL
Our Zoom Sessions – Staff Guidelines

Zoom is one of the most popular video conferencing applications at the moment and it is now being used widely in schools to support teaching during the COVID-19 lockdown.

Zoom can monitor a pupil's activity, allowing a member of staff to track real-time activities, screen-share, record live lessons and recall video, audio, transcript and chat files. This resource is a great way to attempt to replicate classroom learning, however, as with all platforms there have recently been concerns over security but the school will take measures to maximise the use and security whilst utilising Zoom.

Alpha Preparatory School will be using Zoom sessions to complement our online learning platform and every care will be taken to ensure children's safety when engaging in an online lesson or online activity with a member of staff.

- Alpha Preparatory School will ensure the latest version of Zoom is available and this will be updated when any new upgrades become available. These updates will ensure the platform will not be vulnerable to hacking and will maximise security.

- All Zoom lessons will be set up by the Host (i.e. Alpha Preparatory School) using a meeting ID number and entry to the session will be password protected, only allowing those invited to each session to sign in. This is intended to stop the possibility of sessions being hacked by external sources. The password and link will be sent to invitees via an official school email, ending in @alpha.harrow.sch.uk so only those intended to join can access the virtual classroom.

- The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the Host to screen them before entering. This feature will be enabled and pupils will be admitted to the session by the Host. This function adds another layer of security to reduce the likelihood of 'Zoom Bombing'. (unauthorised people joining meetings uninvited and broadcasting inappropriate material).

- Staff members hosting the Zoom sessions must remain aware and vigilant during the online session.

- Once the lesson has started, the Host should 'lock the classroom', meaning no one else can join the session again, protecting the virtual classroom from anyone entering who is not welcome. If a student or another member of staff have been invited to the session, only unlock the room at the time agreed and admit the invitee from the waiting room.

- Privacy controls will be set so that screen sharing is limited to the Host only. This reduces the risk of hacking or the installation of malware.

- When hosting a virtual lesson, staff should dress appropriately and find a setting which has a plain background and has no personal information on display or inappropriate items on show.

- Pupils and parents have been issued with Zoom Guidelines and pupils should be reminded of the guidelines regularly, particularly about what is acceptable behaviour and expected conduct during class. They may need reminding that, despite being at home, the same level of behaviour and conduct exists as if they were at school, such as listening to instructions, to be polite and to remember their manners.

- Pupils should be reminded that inappropriate behaviour may result in them being removed from the session.

- It is up to staff if they wish to video record their session. This is not a requirement of the school unless otherwise stated by the Headmaster.

- If you are hosting a large session, you should pre-set your meeting to mute participant's microphones upon entry. This helps to avoid background noise and allow your students to focus on the session. You may wish to use the 'mute all' facility during your class sessions.

- To create eye contact with pupils, staff should look directly at the camera. This helps to create a more personal connection while teaching over video.

- Staff should speak as though they are face-to-face with the class whilst ensuring they are at the appropriate distance from the microphone giving the best audio experience.

- When delivering a presentation, sharing images, files or video, pupils should be given a moment to open or take in what has been shared.

- Be aware of what is showing on your screen when you are screen-sharing.

- Be aware of your browsing history if looking for a clip whilst screen-sharing etc to support learning, it is best to have any documents or resources open or downloaded prior to the start of the session.

ALPHA PREPARATORY SCHOOL
Staff Agreement for Acceptable Use of the Internet and ICT

The computer network, school laptops and other digital devices are owned by the school and are made available to staff to enhance their professional activities, including teaching, research, administration and management.

- Staff should make themselves familiar with the school's E-safety policy and ensure that they adhere to it.
- Staff will be accountable for any misuse of the school network, computers, laptops or other ICT equipment.
- Staff understand that their use of the school's network is monitored and the school reserves the right to examine or delete files that may be held on its computer network, laptops or other devices. Monitoring data is processed in accordance with the school's privacy notices.
- Staff should not attempt to bypass the school internet filtering system.
- Any internet sites to be used in lessons should be thoroughly checked beforehand - remember to check for inappropriate adverts, comments and links to other sites.
- If a school laptop or other digital device is taken home, staff should ensure that other family members do not use it and that it used only for school business.
- Use of school equipment to access inappropriate materials such as pornographic, racist or offensive material is forbidden. Personal social networking sites should not be accessed using school equipment or used to communicate with pupils.
- Mobile phones and other personal communication devices will not be used during lessons or whilst pupils are present, unless there is an emergency or safeguarding issue.
- Mobile phones/personal equipment should not be used to take pictures or record pupils, unless consent has been authorised by the headmaster.
- Think carefully before printing and ensure it is collected from the printer promptly, so that sensitive information is not left exposed.
- Staff will check their school email account daily and use this account only as described in the E-safety policy.
- Do not leave sensitive data on printers or viewable on your computer screen.
- Keep your login details secure and log off or lock the computer when you are not in attendance.
- Any data concerning pupils should not be taken from the school or stored on a portable device unless it is in line with the security procedures outlined in the E-safety policy.
- Copyright of materials must be respected and sources acknowledged when used.

Staff should seek advice from the Computing coordinators or Headmaster if they are unsure about any point of acceptable use of ICT/equipment.

Name:

Signature: Date:

The documentation below this point is provided to parents on admission to Alpha Preparatory School which they must sign and return to school:

Dear Parent,

Acceptable use of the internet and Information & Communication Technologies (ICT).

As part of the school's computing programme, we offer pupils filtered access to the internet through the London Grid for Learning. This allows pupils to have access to a whole world of learning resources and can significantly enhance the learning experience of our children.

The school's aim for internet and ICT use is to improve learning and teaching, and to work with parents in educating children in the safe and responsible use of these technologies. To this end, we have safeguards in place, such as the use of strong filtering, monitoring procedures and ensuring that all protection software is up-to-date. We have also integrated E-safety learning into the curriculum to help the children recognise and manage risks. We have rules in place to guide the children in acceptable use. However, it must be recognised that no system is 100% perfect and that some unsuitable material may be accessed intentionally or by accident. Immediate remedial action will, of course, be taken if this occurs. However, we believe that the benefits of using the internet in school exceed the potential disadvantages.

Outside of school, families bear the same responsibility for the guidance they exercise with the internet and other communication devices, such as television, gaming devices and mobile phones. As part of our partnership, we have provided a copy of the pupil rules for responsible internet and computer use which have been discussed with the children.

We would be grateful if you would read these rules and sign/return the permission slip to confirm your permission for your child to receive controlled internet access at school.

If you do not give your permission, then internet access for your child will be withdrawn.

ALPHA PREPARATORY SCHOOL
Pupil Rules for Responsible Internet and Computer Use (Year 3 - 6)

I understand that the school has installed computers and internet access to help our learning. The rules below will keep everyone safe and help us be fair to others.

- I will keep the ICT suite tidy when I use it.
- I will look after all ICT equipment.
- I will not bring food or drinks into the ICT suite.
- I will only use the system with my own username and password, which I will keep secret.
- I will only use the computers for school work, educational games and homework.
- I will only print with a teacher's permission.
- I will ask permission from a teacher before using the internet and will only access websites that have been approved by the school.
- I will not bring in storage devices, such as memory sticks or CDs, from outside school unless I have asked my teacher.
- If I find anything I don't like, think a page online is inappropriate or feel uncomfortable with anything online, I will tell my teacher.
- I will not give my home address, telephone number or other personal details or arrange to meet anyone over the internet. Nor will I access other people's files or give out personal information about them.
- I will not use the computers or internet to produce any material or send any message which will deliberately hurt or upset someone
- I will report any unpleasant material or messages sent to me. I know that I can do this confidentially and that this will help to protect others as well as myself.
- I understand that the school monitors my use of school computers, may check my computer files and look at the internet sites I have visited.
- I understand that if I do not behave responsibly my parents will be informed and my computer/internet access may be withdrawn for a period of time.

When you have discussed this form at home, please complete the information and return this whole form to your computing teacher.

PUPIL STATEMENT:

I agree to using the school computers and internet at school safely and responsibly. I have read the rules that are included with this form and these have been explained to me at school. I agree to follow these rules.

Pupil's Name: _____ Year: _____

Pupil's Signature: _____ Date: _____

PARENT/GUARDIAN STATEMENT:

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the internet at school. I understand that pupils will be accountable for their own actions if they intentionally break the rules of acceptable use. I also understand that some materials on the internet may be unsuitable, though the school will use filtered access to control this risk.

Parent's Name: _____

Parent's Signature: _____ Date: _____

ALPHA PREPARATORY SCHOOL
Pupil Rules for Responsible Internet and Computer Use
(Reception and Key Stage 1)

These rules will keep everyone safe and help us be fair to others.

- I will look after all ICT equipment.
- I will only use my own username and password and keep it secret.
- I will only use the school computers for school work and educational games.
- I will only print if I ask the teacher.
- I will ask the teacher for permission before using the internet.
- I will tell my teacher if I see anything I don't like or if I feel uncomfortable with something I see.
- I know my teacher can look at what I have being doing on the computer.
- I understand that if I do not behave responsibly my parents will be informed and I will not be allowed to use the computer for a period of time.

PARENT/GUARDIAN STATEMENT:

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the internet at school. I understand that pupils will be accountable for their own actions if they intentionally break the rules of acceptable use. I also understand that some materials on the internet may be unsuitable, though the school will use filtered access to control this risk.

Parent's Name: _____

Parent's Signature: _____ Date: _____