Olive Tree Study Support

E-SAFETY POLICY (INCLUDING ACCEPTABLE USE POLICY)

INTRODUCTION

This policy has been derived and adopted from Thames View Infants School's e-safety policy by the permission of the Headteacher. This policy should be read in accordance with the school's social networking policy.

PURPOSE

Due to the unregulated nature of the internet, there are risks that children may gain access to material that is inappropriate. This policy sets out the measures to be taken that minimize these risks.

Schools must have an e-safety policy covering the safe use of internet and electronic communications technologies such as mobile phones and internet connected devices. The policy will highlight the need to educate children and their families about the benefits and risks of using new technologies both in and away from the school context. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The schools e-safety will operate in conjunction with other policies including behaviour, bullying, data protection, safeguarding, information security and any home-school agreements.

REMIT

This policy applies to all members of the school (including staff, pupils, volunteers, parents/carer, visitors and community users) who have access to and are users of school ICT systems, both in and out of the school. This is policy pertinent to incidents of cyberbullying, or other e-safety incidents, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Olive Tree Study Support

ROLES AND RESPONSIBILITIES

E-Safety Audit

This audit should be completed by the member of the senior leadership team (SLT) responsible for e-safety policy. Staff who could contribute to the audit includes the Child Protection coordinator, e-safety coordinator, ICT leader and Directors.

Date of latest update of the e-safety policy (at least annual)

The school e-safety policy was agreed by Directors on: June 2016

The policy is available for staff at: School website

The policy is available for parents at; School website

The e-safety coordinator is: Branch Coordinator and Line Manager

The member of the senior leadership team responsible for e-safety is: Harun Rashid

The member of the Directing body responsible for e-safety is: Abdul Alim and Tahera Akther

The Child Protection coordinator is: Branch coordinator and Abdul Alim

Has e-safety training been provided for all staff? Y/N

Has e-safety guidance been provided for all pupils? Y/N

Are e-safety guidance materials available for parents? Y/N

Is there a clear procedure for a response to an incident of concern? Y/N

Have e-safety materials from Main School and other agencies been considered? Y/N

Have all staff teaching and non-teaching signed the acceptable use policy? Y/N

Have all parents/carers signed an e-safety home/school agreement form? Y/N

Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? Y/N

Is personal data collected, stored and used according to the principles of the data protection Act? Y/N

Has filtering on internet-based devices been appropriately applied? Y/N

The school encourages use by pupils of the rich information resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our pupils will be entering.

Access to online resources will enable pupils to explore thousands of libraries, databases and bulletin boards while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to such information resources and increased opportunities for collaboration exceed the disadvantages. However, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school (in some cases the roles described may be combined).

HEADTEACHER:

To take overall responsibility for e-safety provision

To take overall responsibility for data and data security.

To ensure that school uses an approved, filtered internet service which complies with current statutory requirements.

To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues as relevant.

To be aware of procedures to be followed in the event of a serious e-safety incident

To receive regular monitoring reports from the e-safety coordinator/officer

To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures e.g. network manager.

E-SAFETY COORDINATOR (Lead Branch Coordinator):

To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies/documents.

To promote an awareness and commitment to e-safeguarding throughout the school community.

To ensure that e-safety education is embedded across the curriculum

To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

To ensure that an e-safety incident log is kept up to date.

Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues.

To facilitate training and advice for all staff.

To liaise with the local authority and relevant agencies.

DIRECTORS:

To ensure that the school follows all current e-safety advice to keep the children and staff safe

To approve the e-safety policy and review the effectiveness of the policy.

To support the school in encouraging parents and the wider community to become engaged in e-safety activities.

The role of the e-safety Director will include regular reviews with the e-safety coordinator/officer including e-safety incident logs, filtering/change control logs.

NETWORK MANAGER/TECHNICAL STAFF/ICT LEADER (Harun Rashid):

To report any e-safety related issues that arises, to the e-safety coordinator

To ensure that users may only access the schools networks through an authorized and properly enforced password protection policy, in which passwords are regularly changed.

To ensure appropriate back up procedures exist so that critical information and systems can be recovered in the event of a disaster.

To check filtering lists are reviewed on a regular basis

That the use of the network/internet/email to regularly monitor in order that any misuse/ attempted misuse can be reported for investigation.

To keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

TEACHING AND SUPPORT STAFF:

To ensure that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

To read, understand, sign and adhere to the school staff acceptable use agreement/policy

To embed e-safety issues in all aspects of the curriculum and other activities

To report any suspected misuse or problem to the e-safety coordinator.

To ensure that any digital communications with pupils and parents should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

To supervise and guide pupils carefully when engaged in learning activities involving online technology including extra-curricular and extended school activities if relevant.

To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

To be aware of e-safety issues to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

To maintain an awareness of current e-safety issues and guidance e.g. through CPD

To model safe, responsible and professional behaviours in their own use of technology

PUPILS

To read, understand and follow the e-safety rules

To understand the importance of reporting abuse, misuse or access to inappropriate materials and how to do so.

To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

To know, understand and adhere to the school policy in the use of mobile phones, digital cameras and hand held devices, including of images and cyberbullying.

To understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the schools E-safety policy covers their actions out of school, if related to their membership of the school.

PARENTS/CARERS

To support the school in promoting e-safety and endorse the parents acceptable use agreement, including the use of photographs and video images.

To read, understand and promote the school pupil acceptable use agreement with their children

To consult with the school if they have any concerns about their children’s use of technology.

GUIDELINES

The following guidelines state appropriate procedures for implementing the above policy and for reviewing and evaluating its effect on teaching and learning.

Education-Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating the pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of any school's e-safety provision. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum in the pupils week day school, staff therefor should reinforce e-safety message that are taught in the week day schooling system.

Key e-safety messages should be reinforced as part of the Islamic Studies programme activities.

Pupils should be reinforced the school rules for children using the internet safety.

Pupils should be encouraged to adopt a safe and responsible use of technology both within and outside school, including appropriate online behaviour and keeping personal information private.

Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

EDUCATION AND TRAINING- STAFF AND DIRECTORS

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Directors are invited to e-safety training events.

Training will be offered as follows:

All staff should receive e-safety training as part of their induction programme. Ensuring that they fully understand the school e-safety policy, acceptable use agreements and social networking policy.

The e-safety coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations.

This e-safety policy will be presented to and discussed by staff in staff meetings

The e-safety coordinator will provide advice/guidance/training to individuals as required.

EDUCATION-PARENTS/CARERS.

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in education of their children and in monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore need to reinforce information and awareness to parents and carers through:

Letters, newsletters, website

Displays in school/ at parents meeting

Reference to the relevant websites/publications for further support.

RESPONSIBILITY OF PARENTS.

Parental involvement can help reinforce the messages of internet safety and extend the learning progress into the home. As well as returning the internet permission slip and Image Consent Form, parents are sent home a copy of the parent's Guide to the internet.

PARENTAL PERMISSION:

Internet Usage

No pupil should use the internet without parental permission, and without accepting the school's rules on Acceptable Use which will form part of home-school partnership agreement. This acknowledges that parents and carers accept some responsibility for the way in which their children use the internet and that in spite of all reasonable precautions and supervision there still remains a small risk of children viewing inappropriate material.

Photographs and Video of Pupils:

All parents are required to complete and return the image consent form, which will also form part of the home-school partnership agreement. This allows the school to take photographs and video of the children for use within the school website, twitter and YouTube pages.

A Common-sense Approach:

Many of the risks of using the internet and related technologies can be minimized by taking a common sense approach:

Sitting computers in areas with open access, where everyone can see what is on the screen

Taking an interest in the internet and regularly discussing what children see and use

Monitoring online time and being aware of the nature of the work being completed on the web.

Educating children to use the internet in a sensible and responsible manner

Making pupils aware of the importance of not divulging personal information such as name, address and phone numbers on the internet.

Encouraging learners to be critical users of the internet: “is the information true? How do you know?”

Warning children that there are some unsuitable sites on the internet and discussing the issues involved.

Making the children clear of the consequences for misuse of the internet and technologies present in the school.

Pupils will be reinforced how to respond to the dangers of encountering inappropriate content, cyberbullying and grooming are explored. This would include, for example:

Saying no

Exiting a screen

Telling an adult straight away

Supervision

Pupils must be supervised when using a computer. Within communal areas like halls and corridors, it is accepted that children might not be supervised directly and that nearby staff will share this responsibility.

Responsibilities of children;

The school has developed a set of guidelines for internet use by pupils. All children must be taught about acceptable and responsible use of the internet and should be aware of these class rules:

RULES FOR USING TECHNOLOGIES IN SCHOOL:

I can only use the internet at school or at home if my parents agree.

I must ask permission from a teacher before using the internet in school.

I can only use computers at break and lunch times if a teacher is nearby.

I must keep my logins and passwords secret.

I am responsible for taking care of the computers and ICT equipment

I must ask for help from a teacher, or other suitable adult, if I am unsure what to do or if I think that I might have done something wrong

I must not look at other people's file without permission

I am only allowed to delete my own files.

I am not allowed to answer a face time call or reply to a text/chat message/e-mail at school unless it's part of a lesson.

I know that staff will never call, text, chat or email me, whether in school or outside school unless it's part of the lesson.

I will only use the schools computer for school and homework.

I will only send messages that are polite and sensible.

I will never give out personal information, nor send photographs or videos to people I don't know or trust even at home.

If I see anything unpleasant in the internet I must sensibly exit the screen, turn the monitor off and tell an adult right away.

I know that if I break the rules, I might not be allowed to use a computer.

PERSONAL DEVICES:

Personal devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

Staff should not use their personal device when contacting pupils or parents, there should be access to a school phone.

Pupil's mobile phones should not be brought in to school.

The recording, taking and sharing of images, video and audio on any personal device is to be avoided, except where it has been exactly agreed otherwise by the Headteacher.

The school reserves the right to search the content of any mobile or handheld device on school premises where there is a reasonable suspicion that it may contain undesirable material.

Personal devices will not be used during lessons unless as part of an approved and directed curriculum-based activity.

Olive Tree Study Support

Below are linked to the e-safety in computing programme of study and are addressed through everyday teaching and school based training for parents:

Chat-rooms, discussion groups, social networks and instant messaging like Facebook messenger: children are not allowed to access the above within school. To decrease the risk of children accidentally stumbling upon these, staff are required not to log on to chat rooms, join discussion groups or any other platform within school. Facebook should not be used by anybody under the age of 13.

Real time conferencing (face time/Skype/IMO): this should only take place within the school under direct adult supervision during lesson time.

Email:

Children are not allowed to access their home-based email accounts within the school. Children will be reminded not to divulge personal information via e-mail and will be warned of the dangers of:

Bullying

Anonymous senders

Spam

Grooming and exploitation, racist/hateful/extremist and other illegal content which are anti-British value.

RESPONSIBILITIES OF STAFF:

All staff teaching and non –teaching must be made aware about acceptable and responsible use of the internet and should be made aware of school guidelines on the matter. Irresponsible use of the internet jeopardizes the safety of children.

Inappropriate Materials

Staff teaching and non-teaching must never knowingly seek to view material over the internet that is illegal, pornographic, sexist and racist, or in any way offensive to minorities or that would be considered unsuitable within a school environment or infringes the school's equality plan and community cohesion-ethos. This includes but it is not limited to material of an illegal sexual or offensive nature including any radicalized, terrorist or extremist political or religious viewpoint that may bring the school or the local authority into disrepute. It is acceptable to use the inter net in school for social or personal activities but not for e-commerce.

Photographs of children (in the 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 and pupils need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

Parents/guardians should sign the consent form before taking photographs which takes place as part of the admissions process and the home school agreement, which should be reviewed annually.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, publication, sharing and distribution of images.

Children on School Websites:

It is the schools duty to ensure that every child in their care is safe and accordingly, it's important that no individual child is able to be identified by visitors to the school's website. Pupil's full names will not be used anywhere on a website, twitter or blog, unless with the permission of the parents. Consequently, the school website, twitter or blog should not include:

Photographs of individual children, instead use only group or whole class images with very general labels such as Arabic lesson.

Personal details or names of any child in a photograph

In accordance with guidance from the information commissioner's office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use.

Staff will not take pictures of children using their own personal devices except when use for a school-authorized Facebook account. Where this is the case, the staff member MUST ensure that all pictures of children are removed at the end of the day.

Chat-rooms, Discussion Groups and Instant Messaging (Facebook messenger):

As noted above, in order to decrease the risk of children accidentally stumbling upon these, staff are required not to log on to chat rooms, join discussions or use any form of instant messaging within school.

E-mail:

Staff should not check their email accounts at school. This is due to pornographic spam and unsuitable pop-up windows associated with such sites. After checking their school emails, staff are asked to ensure that they have fully logged out from their email programme.

Downloading Files and Attachments and Virus Awareness:

In order to protect the resources of the school, staff should be aware of anti-virus practices. To avoid the risk of virus infection, teachers are requested not to download any programme from the internet onto any school-based machine. Staff are asked to be aware of hidden viruses when opening e-mail attachments; passwords will need to be divulged to those concerned.

Data protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

Fairly and lawfully processed

Processed for limited purposes

Adequate, relevant and not excessive.

Accurate

Kept no longer than is necessary

Processed in accordance with the data subject's rights

Secure

Only transferred for others with adequate protection.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Ac 1998 and other relevant legislation.

The head teacher is the senior information risk officer

Staff must ensure that at all times they take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.

Staff must use personal data only on secure password protected computers and other devices, ensuring that they are properly logged off at the end of any session.

Staff must ensure they only transfer data using encryption and secure password protected devices.

PROJECTOR HEALTH AND SAFETY ISSUES.

It is important that all users are aware of the health and safety implications of using projection equipment in the classroom, particularly if children might stand in front of a beam to give presentations. All projectors have the potential to cause eye injury; so some simple guidelines should be followed;

No one should stare directly into the beam of the projector. Children should be reminded of this danger.

The use of a stick or a laser pointer is recommended to avoid the need for the user to enter the beam.

Teachers should undertake a risk assessment of children's behaviour and sensibility when allowing them to work without direct supervision, in an area with a projector.

Projectors should be installed as far as forward as possible to avoid the projector beam entering the user's field of vision.

Electrical standards and regulations apply to all interactive whiteboards aspects.

Appropriate lighting is very important. Control the light in the room by using blinds, which diffuse rather than move ambient lighting; thus reducing the need to increase the beam intensity.

Retaining some ambient light enables eye to eye contact to be maintained. There is some evidence that pupils work more ably when exposed to natural light. Restore natural daylight as soon as possible.

COMMUNICATIONS;

A wide range of rapidly developing communications technologies has the potential to enhance learning. Schools need the benefit of using these technologies for education whilst reducing their risks:

Pupils may only use email accounts on the school system which are approved by the school.

Pupils must immediately tell an appropriate member of staff if they receive any offensive email.

Staff should only use their school email account in communication with pupils and parents

In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

Pupils need to be educated in how to deal with incoming email and association attachments.

The school should consider how email from pupils to external bodies is presented and controlled.

Staff should only use their school email account in any communication relating to school business.

SOCIAL MEDIA –PROTECTING PROFESSIONAL IDENTITY

All schools have a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place and these are stated within the schools social Networking Policy.

The school has a clear reporting guidance, including responsibilities, procedures and sanctions.

All schools staff sign the acceptable use policy indicating they understand and will follow the guidance contained

School staff ensure they make no reference in social media to pupils, parents/carers or school staff.

School staff should ensure that personal opinions are not attributed to the school or local authority.

School staff should ensure that security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information.

SOCIAL MEDIA-PUPILS;

The school will control access to social networking sites and where relevant educate pupils in their use.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location

Pupils and parents will be advised that the use of social networks spaces outside school brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

RESPONDING TO INCIDENTS:

Complaints of internet misuse will be dealt with by a senior member of staff

Any complaint about staff misuse must be referred to the Headteacher.

Complaint of a child protection nature must be dealt with in accordance with school child protection procedures.

If a member of staff or pupil receives online communication that is considered particularly disturbing or illegal, the Police will be contacted.

Monitoring of incidents takes place and contributes to developments in policy and practice in e-safety within the school.

Parents/carers are informed of e-safety incidents involving children and young people whom they are responsible.

Olive Tree Study Support

STAFF ACCEPTABLE USE AGREEMENT FORM

I understand that I must use school ICT systems in a reasonable way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognize the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

I understand that statements set out in this agreement also apply to use of school ICT systems like laptops, email, VLE among others, outside school, and to the transfer of personal data out of school.

I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal use with the policies set down by the school.

I will not disclose my username or password to anyone nor will I try to use any other person's username or password. I understand that I should not write down or store a password where it is possible that someone may steal it.

I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person, including concerns I have regarding radicalization of pupils or colleagues

I understand that the school may monitor my use of the ICT systems including email and other digital communications.

I will adopt the advice given within the schools social Networking Policy.

I will be professional in my use of school ICT systems:

I will not access copy, remove or otherwise alter any other user's files without their express permission.

I will communicate with others in a professional manner; I will not use aggressive images and I appreciate that others may have different opinions.

I will not use personal digital cameras or phones for taking pictures or transferring images of pupils or staff, images will only be taken in accordance to the school guidelines.

I will not connect a computer to the network/internet that doesn't have up to date anti-virus software and I will keep any loaned equipment up to date, using the school's recommended anti-virus system.

I will not connect a USB flash drive to the school network if it has been use on a home computer without up to date anti-virus software.

I will communicate with pupils and parents using official school systems.

I will not engage in any online activity that may compromise my professional responsibilities.

I will not browse, download or send material that could be considered offensive or obscene.

I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.

Olive Tree Study Support

I will ensure that I and any classes am responsible for, treat the school equipment appropriately when using, transporting and storing it.

Where work is protected by a copy right, I will not download or distribute copies including music, videos and images.

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

To protect my personal integrity:

I will ensure that any private social networking sites that I create or actively contribute to are not in conflict with my professional role.

I will ensure that no reference is made in on social media to pupils/carers or school staff.

I will not engage in any one activity that may compromise my professional responsibilities.

Personal opinions should not be attributed to the school.

I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities,

I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action

I understand that it is my responsibility to ensure that I remain up-to-date and understand the school's most recent E-safety Policy.

I agree to abide by this Acceptable Use Policy.

SIGNED…… FULL NAME…….

JOB TITTLE……. BRANCH …….

DATE…….

Olive Tree Study Support

PARENT/CARER ACCEPTABLE USE AGREEMENT FORMS

PERMISSION FORM

Our children all know how to be safe when online when in school and at home. We teach this message regularly to children. We have very comprehensive school policies, all available on our school website, which stipulate how we do this. Together we need to continue to be vigilant with our children to recognize and avoid e-safety risks and to build children's resilience.

The internet does indeed contain material that can harm children if left unsupervised: inappropriate age-related content, prejudice, racism, sexism, homophobia, violence, terror and illegal content of an extremist nature, which undermines our core values as British citizens. Unsupervised access to the internet can put children at risk of bullying or even grooming via email/text/chat clients. The main educational providers try to filter known offensive location materials of this kind, but there is too much for this filtering to be completely be effective, and the locations change frequently. Blocking access to this kind of material by having a restricted range of pages available can also be problematic. An alternative system is to educate pupils and parents about e-safety and encourage an Acceptable Use Policy and partnership between home and school to ensure children remain safe.

The internet does indeed contain material that can harm children if left unsupervised: inappropriate age-related content, prejudice, racism, sexism, homophobia, violence, terror and illegal content of an extremist nature, which undermines our core values as British citizens. Unsupervised access to the internet can put children at risk of bullying or even grooming via email/text/chat clients. The main educational providers try to filter known offensive location materials of this kind, but there is too much for this filtering to be completely be effective, and the locations change frequently. Blocking access to this kind of material by having a restricted range of pages available can also be problematic. An alternative system is to educate pupils and parents about e-safety and encourage an Acceptable Use Policy and partnership between home and school to ensure children remain safe.

Together, therefore it is important that we ensure that our children are as possible when using this type of technology and teach them like other aspects of life to be safe and to share with an adult when things aren't right.

Accordingly, we all have a duty to:

Protect our children from on line bullying, inappropriate age-related content, prejudice, racism, sexism, homophobia, religious or political extremism, violence, terrorism and on-line grooming.

Teach children how to be safe, monitor their online usage, support them when they require help and be a good role model.

Ensure children do not use their technologies excessively, unsupervised and without clear boundaries/time-frames and with consequences if rules are broken.

Agree to a code of conduct "An Acceptable Use Policy for internet use.

We have a set of rules which our children should adhere to, both at school and at home and we need our parents/guardians to ensure that children understand these guidelines and that they stick to them.

ICT including the internet, e-mail and mobile technologies is becoming more and more of an integral part of society and it is important that we work together that our children grow up knowing how to use

all of this technology safely and confidently. We have designed this agreement to highlight our commitment to ensuring your child's safety in partnership with yourselves.

If you have any concerns or would like to discuss this matter any further, please come in and speak with us.

Yours sincerely

……

Tahera Akther

Headteacher

PARENT/CARER ACCEPTABLE USE AGREEMENT FORM FOR HOME-USE DEVICE

Parent/carer copy

Parent/carer name:		Relationship:	
Pupil name:			

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's safety.

I will not tell my child password nor allow them to download any apps.

I will ensure that my chosen site engines have strict filtering set.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems to ensure that young people will be safe when they use internet and ICT systems.

I understand that at school, my child's activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use policy.

I understand that I must actively monitor my child's use of their device and internet access too.

I understand that an I-pad doesn't substitute a meaningful conversation with an engaged adult.

I understand that unrestricted I-pad use can harm a child and cause obsessive behaviours.

I understand that children should not have access to Facebook/instagram/twitter and any other social media applications that are not age appropriate. Any applications of this nature will be removed from any I-pads taken to school. I understand that allowing children to access age-inappropriate material is regarded as a safeguarding matter and will be reported as such.

I will support the school in reinforcing the school's online rules.

Olive Tree Study Support

RULES FOR USING TECHNOLOGIES IN SCHOOL:

I can only use the internet at school or home if my parents agree.

I must ask permission from a teacher using the internet in school.

I can only use the computers at break and at lunch if a teacher is nearby.

I must keep my log-ins and passwords secret.

I am responsible for taking care of the computers and ICT equipment.

I must not look at others people's files without their permission.

I am only allowed to delete my own files.

I am not allowed to answer a Face time call or rely to a text/chat message/ email at school unless it is part of the lesson.

I know that staff will never call, text, chat or email me, whether in school or outside school.

I will only use the schools computer for school and homework.

I will only send messages that are polite and sensible.

I will never give out personal information, nor send photographs or videos to people I don't know or trust even at home.

If I see anything unpleasant in the internet I must sensibly exit the screen, turn the monitor off and tell an adult right away.

I know that if I break the rules, I might not be allowed to use a computer.

Pupil Signed:	
Dated:	

Olive Tree Study Support

USE OF DIGITAL/VIDEO IMAGES

Parent/Carer name:
Pupil name:

The use of digital/video images plays an important role in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school.

In accordance with guidance from the information commissioner's office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use as such use is not covered by the Data Protection Act.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children.

As the parent/carer of the above pupil, I agree to the school taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

YES/NO

I agree that if I take digital or video images at or of, school events which include images of children other than my own, I will abide by the guidelines above in my use of these images.

YES/NO

Signed :

Date: