Oaktree Nursery and Primary School Online - Safety 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.

Rationale

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning, therefore safe internet access should be encouraged in the school community. Children should be taught how to use an array of devices and online benefits effectively and learn the skills that allow them to be responsible and safe online citizens. Some of the risks they may face are:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children on the potential risks.

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of; pupils / pupils' parents / carers / staff

This online-safety policy was approved by the *Governing Body on:*	March 2021
The implementation of this online-safety policy will be monitored by the:	Computing Coordinator, Online Safety Lead and SLT
Monitoring will take place at regular intervals (see note below):	
The *Governing Body* will receive a report on the implementation of the online-safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually in the Autumn Term
The Online-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online-safety or incidents that have taken place. The next anticipated review date will be:	September 2021
Should serious online-safety incidents take place, the following external persons / agencies should be informed:	Swindon Borough Council ICT Manager/Safeguarding Lead, South West Grid for Learning Safeguarding Officer and, should it be deemed necessary, the Police

Roles and Responsibilities

The following section outlines the online-safety roles and responsibilities of individuals and groups within the school:

The Online safety Co-ordinators: Computing Coordinator, The Headteacher and Designated Safeguarding Lead

- Form part of an online-safety committee that takes day to day responsibility for online-safety issues
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online-safety incident taking place
- Provide training and advice for staff and parents
- Liaise with the Local Authority
- Liaise with school ICT technical staff (GHS) and internet service provider (SWGFL)
- Receives reports of online-safety incidents and creates a log of incidents to inform future online-safety developments
- Meet with Governor responsible for online-safety, to discuss current issues, review incident logs and filtering/change control logs
- Attend necessary training to enable them to carry out their online-safety roles and to train other colleagues, as relevant.

Governors

Governors are responsible for the approval of the Online-Safety Policy and for reviewing the effectiveness of this policy. This is carried out by the FGB, who receive regular information about online safety incidents and monitoring report. The Safeguarding Governor has taken on the role of Online-Safety. This role includes:

- meetings as required with the Online-Safety Co-ordinator
- attendance at Online Safety Group meetings
- monitoring of Online safety incident logs
- monitoring of filtering / change control logs
- reporting to relevant Governors

Network Manager

The Network Manager is responsible for ensuring:

- that the technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Online Safety lead.
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff Responsibilities

Staff are responsible for ensuring that:

- They have an up to date awareness of online-safety matters and of the current school online-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy
- They report any suspected misuse or problem to the IT Coordinator for investigation
- Digital communications with pupils should be on a professional level and only carried out using official school systems (Microsoft Office 365) with documents encrypted where necessary
- Online-safety issues are embedded in *all* aspects of the curriculum and other school activities
- Pupils understand and follow the school online-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor IT activity in lessons, extra-curricular and extended school activities
- They are aware of online-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and adhere to current school policies with regard to these devices
- In lessons, where internet use is pre-planned, pupils take part in a discussion about safe search terms for their research and make appropriate responses to any inappropriate materials found on the internet.
- They act as good role models in their use of digital technologies, the internet and mobile devices

Designated Safeguarding Lead

The DSL is trained in online-safety issues and is aware of the potential for serious Safeguarding and Child Protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand the school's policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online-safety practice when using digital technologies out of school and realise that the school's Online-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and providing information about national/local online-safety campaigns. Parents and carers will be encouraged to support the school in promoting good online-safety practice and to follow guidelines on the appropriate use of:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website, VLE and other online resources provided by the school in accordance with the Pupil Acceptable Use Policy signed by pupils / parents on entry to the school and upon entering a new key stage.

Online-Safety education is provided in the following ways:

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

Online-safety is a safeguarding concern and teachers and learning assistants reinforce online-safety messages across the whole curriculum. The online-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities. It is provided in the following ways:

Educating Pupils

- Key online-safety messages are delivered in an annual assembly during the Spring Term, to coincide with 'Safer Internet Day'
- Key messages are reinforced in lessons across the curriculum throughout the academic year
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are frequently reminded of the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Where internet use is pre-planned, pupils use websites recommended by teachers or have discussed appropriate search terms
- Children further up the school have a strong understanding of how search results are generated and the order in which they are presented.

Educating Parents / Carers

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 therefore seeks to provide information and awareness to parents and carers through:

- Sending relevant documentation detailing updated online-safety information, alerting parents / carers to both existing and new dangers children are faced when accessing on-line / mobile technologies
- Alerting them to the 'Pupils' Acceptable Use Agreement' at parents' meetings
- Notifying them of incidents concerning their children
- Providing a monthly digital newsletter written by the digital leaders and online safety coordinator
- Targeted and relevant parent information sessions held in school and hosted by the Online Safety Coordinator at least twice yearly.

Educating Staff

All staff receive annual online-safety training to help them understand their responsibilities, as outlined in this policy and keep them informed of up to date campaigns / literature.

- A planned programme of formal online-safety training is made available to staff. This is regularly updated and reinforced. An audit of the online-safety training needs of all staff is carried out annually
- All new staff receive online-safety training as part of their induction programme, ensuring that they fully understand the school online-safety policy and Acceptable Use Agreements
- The Online Safety Coordinator receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This online-safety policy and its updates have been presented to and discussed by staff in meetings. This is documented by our safeguarding platform (CPOMS)
- The Online Safety Coordinator provides training to individuals as required.

Governors

Governors take part in online-safety training. This may be through:

- Attendance at training provided by the Local Authority or at an organised SWGfL events
- Participation in school training for staff or parent information sessions (this may include attendance at assemblies / during lessons).

Technical – equipment, filtering and monitoring

The school has a managed IT service proved by GHS and internet services provided by South West Grid for Learning. It is therefore the responsibility of the school to ensure that the managed service provider is fully aware of the school Online-Safety Policy and Acceptable Use Agreements.

The school is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements.
- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- The school Network Manager (GHSUK) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering / monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.
- The Network Manager regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed (see appendix).

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Removable media (eg memory sticks / CDs / DVDs), if still being used, by users on school devices must be safely encrypted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. Personal devices are permitted to connect to the schools wireless network via a guest account but they are not permitted to connect to the school server. In the case of trainee teachers, students or supply teachers, a school device will be loaned to them for the duration of their time in school.

Digital videos and images

The school will educate all it's members on the potential risks associated with taking, sharing and storing images and ensure guidance laid out in this policy is adhered to:

- When using digital images, staff must inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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. To respect everyone's privacy and in some cases protection, parents/carers are made aware that these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes and images must be immediately deleted once uploaded.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, if this is at the request of parents or carers.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupils' work can only be published with the permission of the pupil.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current Data Protection Legislation. Oaktree Nursery and Primary School will ensure that data is:

- 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 to others with adequate protection.

At all times staff must:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- 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 in which they are using personal data
- Use encryption and secure password protected devices to ensure the transfer of sensitive data

W**hen personal data is stored on any portable computer system, USB stick or any other removable media:**

- Data must be encrypted and password protected
- Devices must be password protected
- Devices must offer approved virus and malware checking software
- Data must be securely deleted from the device, once it is no longer needed.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service (Microsoft 365) is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Children are encouraged to leave mobile phones and other personal devices at home, however if children do bring them into school they must be left in the school office.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media mustn't be used for these communications.
- Pupils are taught about online-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference is made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

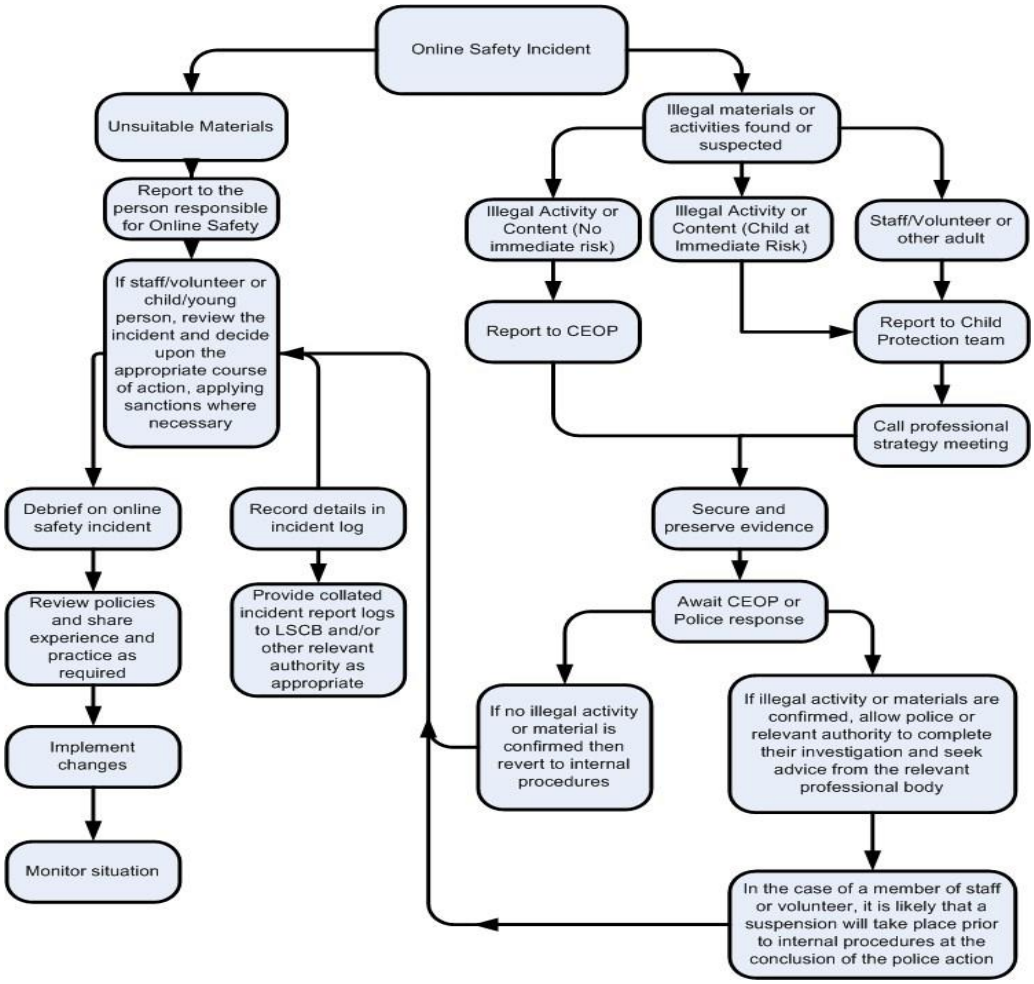
The school's use of social media (Twitter) for professional purposes will be checked regularly by the Online Safety Coordinator and Safeguarding Lead Governor to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Responding to online-safety Incidents

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Online-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the Online-safety Co-ordinator and recorded in the online-safety incident log. The flowchart below should be followed.

Some incidents may need to be recorded in other places, in line with other policies, if they relate to a bullying or racist incident. If any apparent or actual misuse appears to involve illegal activity ie.

- Child sexual abuse images
- Adult material which potentially breeches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct activity or material


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Online Safety Addendum September 2020

Remote Learning

Oaktree Nursery and Primary School recognises the additional risks to pupils and staff associated with spending more time online during the pandemic and periods of remote learning. During this time, our expectations of staff and pupils remain the same regarding the principles and practices set out in the school's Online Safety Policy, Safeguarding Policy and the Acceptable Use Policies. In order to ensure the safety and welfare of children during remote learning, the school will follow the DfE Guidane for Remote Learning.

Throughout any periods of remote learning, we will:

- Continue to remind our children and their parents and carers of what they can do to keep safe online during this time (see below nb)
- Deliver online Safety lessons remotely via Microsoft Teams, or in the form of a work pack in instances where remote learning is not being accessed
- Inform parents about our filtering in school and advise adequate filtering and parental controls on home broadband and mobile networks
- Insure all school devices are regularly updated with the latest software and security settings
- Review the Online Safety Policy and ensure practices are followed, especially in instances of staff delivering remote learning sessions from home.

Parents will be made aware of the following resources available to help develop conversation with their child regarding a healthy online experience; Childnet convestaion starters and more specific guidance for under fives; UKCIS guidance on minimising risk online and the valuable resource Think you Know guidance for parents/carers.

Microsoft Teams

Microsoft Teams is our chosen platform for remote learning; The following measures are in place to ensure the safety of pupils and staff:

- Children are issued with individual logins and instructed to reset passwords upon initial login and personalise according to our password policy
- Children follow behavioural rules and expectations set out by the teacher in the initial online sessions and then revisited in subsequent lessons. These include, switching backgrounds off during recorded sessions, pupils not taking own recording or screen shots of live sessions which include other pupils, being appropriately dressed for online sessions and ensuring that the chat, if used, is used appropriately
- Regularly revisit online safety content during sessions where appropriate and relevant
- Review the security settings on any smart devices being used by staff to deliver remote learning.

Devices on Loan

Devices that are loaned to children during any periods of remote learning are set up using the children's Microsoft 365 account. These devices will be subject to any filtering that is in place in school. Children and parents are reminded of the 'Acceptable Use Policy' and are required to sign a user agreement before the devices are issued.

Online-safety Policy Appendix 1

Pupil Acceptable Use Agreement (KS1)

My teachers will help me learn how to use technology safely, including phones, laptops and tablets.

This is how I stay safe when I use computers:

- I will keep my passwords secret.
- I will only use the computer for things my teacher has told me to.
- I will make sure that when I send messages they are respectful.
- I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.
- I will not reply to any nasty message or anything that makes me feel uncomfortable.
- I will share personal information online.
- In school, I will only use my school email.
- I will not upload photos of myself or any other pupils.
- I understand that these rules are in place to keep me safe online and help me become a super digital citizen.

Signed (child):……

Signed (parent): ……..

Online Safety Policy Appendix 2

Acceptable Use Pupil Agreement (KS2)

My teachers will help me to become a responsible and safe digital citizen. I am responsible for following this agreement to ensure my safety whilst using technolology in school and at home.

Rules and responsibilities for my own personal safety:

- I will only use technology in school for my tasks that have been set by my teacher.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- When communicating online, I will be respectful.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using technology because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online-Safety.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil	
Class	
Signed	
Date	

Appendix 3

Parent / Carer Acceptable Use Agreement

As you will be aware, digital technologies have become fundamental to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and allow greater communication. Young people have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that pupils are responsible and safe digital citizens
- that parents and carers are aware of the importance of online-safety and are involved in the education and guidance of pupils with regard to their on-line behaviour and work in unison with the school.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will in return expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name		Pupil Name	

As the parent / carer of the above *pupil*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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 the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the school systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will reinforce the schools' safe practices in technology use at home and will inform the school if I have concerns over my child's online-safety. I will ensure adequate filtering is in place at home to keep my child safe while using technology at home.

Signed		Date	

Appendix 4

Staff Acceptable Use Agreement (including use of social networking sites.)

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices feature positively as part of our daily working life in school. This policy sets out guidelines in order to make staff aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this user agreement and adhere to its contents at all times. However, the internet involves fast moving technologies and it is impossible to cover all circumstances. Therefore, teachers are required to demonstrate good use of initiative if a situation should arise that might put their professional responsibility into question.

The intention of this guidance is not to stop staff from conducting legitimate activities on the internet, nor to stifle constructive criticism but serves to highlight those areas in which problems can arise for both individual staff members and the School.

There have been several cases where staff have been dismissed by their employer for inappropriate use of technology, in particular use of social website/s or other media.

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
- Access offensive websites or download offensive material.
- Copy information from the Internet that is copyright or without the owner's permission.
- Place inappropriate material onto the Internet.
- Send e-mails that are offensive or otherwise inappropriate.
- Disregard my responsibilities for security and confidentiality.
- Download files that will adversely affect the security of the laptop and school network.
- Access the files of others or attempt to alter the computer settings.
- Update web pages, etc. or use pictures or text that can identify the school, without the permission of the head teacher.
- I will not install any hardware or software without speaking to the ICT technician.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Oaktree Nursery and Primary School.

2. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
3. If I have to use removable media (this should be a last resort), I will ensure that it is adequately encrypted.

4. I will ensure that personal data (such as data held on MIS software) is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely.
5. I will use my school email address only for school related correspondence. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the School's technician.
6. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
7. I will report immediately to the head teacher any unpleasant material or messages sent to me.
8. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
9. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
10. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
11. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

12. I will support and promote the school's online-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

13. Images of pupils and/or staff will only be taken, stored and used for professional purposes, in line with the school mobile phone and camera policy and will only be distributed with consent of the parent/carer or staff member.

The following guidelines have been specifically devised in relation to social networking and should be adhered to at all times. Staff at Oaktree Nursery and Primary School should not:

1. Reveal confidential information about our pupils, staff, or the school or LA
2. Engage in activities on the internet which might bring Oaktree Nursery and Primary School or LA into disrepute
3. I will not give out my own personal details, such as mobile phone number and personal e-mail address to pupils. This includes making 'friends' with children on social networking sites.
4. Use the internet in any way to attack or abuse colleagues

5. Post defamatory, derogatory or offensive comments on the internet about colleagues, pupils, stakeholders or their work at Oaktree Nursery and Primary School
6. Be mindful of the personal information they disclose on social networking sites, especially with regards to identity theft. Making such information as your date-of-birth, your place of work and other personal information publicly available can be high risk in terms of identity theft
7. Make any reference to Oaktree Primary and Nursery school, its pupils or employees. If a staff member is contacted by the media about posts they have made on a social networking site that relates to Oaktree Nursery and Primary School, they should ensure that they talk to the Head Teacher immediately and before responding.
8. Under no circumstances should offensive comments be made about colleagues, School business or stakeholders on the Internet. This may amount to cyber-bullying and could be deemed a disciplinary offence.

Name.....

Signature: .....

Date: .....