



E-SAFETY POLICY

Reference: FIR.SP.001

Approval date: 26th November 2018

Review date: November 2021

Fir Tree Junior School

Radnor Road
Wallingford
Oxfordshire
OX10 0NY



Fir Tree Junior School E-Safety Policy

We are living in an increasingly connected technological world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in E-safety can mean children are unaware of the unintended consequences of their online behaviour or actions. It highlights the need to educate our children and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to keep safe and to control their online experience.

'Our vision is to make the children at Fir Tree School as safe and productive in the online world, both in school and outside of school, as they are in the real world with particular focus on protection against cyberbullying and grooming'.

This policy is intended for our, children, staff, parents, governors, volunteers and visitors.

1. What is E-Safety?

E-safety is a school's ability to **protect and educate** its children and staff in their use of technology as well as having appropriate mechanisms in place to **respond** to and support any incident where appropriate. At Fir Tree, we aim to **protect and educate** our children and will **respond** to incidents where children's safety may be at risk.

1.1 Protect

Protecting children means; providing a safe learning environment by using appropriate monitoring and filtering to control what children can access while at school. Education around e-safety is the only way to ensure that, wherever they are, they know how to stay safe online.

1.2 Educate

Learning about e-safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally, it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, or mitigate the possibility of risk.

The School's E-safety covers a wide range of aspects, including:

- Online behaviour – understanding what constitutes cyber-bullying, inappropriate content and how to behave safely and with respect for others.
- Protecting your online reputation – understanding both the risks and rewards of sharing personal information online (your digital footprint).
- Learning to evaluate internet content – understanding how to research, evaluate and use published material

1.3 Respond

Responding to issues is both about ensuring children know what to do if anything happens to put their online safety at risk, and taking direct and immediate action as a school where incidents occur.

Fir Tree Junior School has clear and robust policies and procedures to identify and respond to e-safety risks or incidents, efficiently and consistently.

The internet is an essential aspect of learning across all walks of life. In school, access to the internet is essential to:

- Raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Prepare children for life in the 21st century in terms for education, business and social interaction. The school has a duty to provide children with quality and safe internet access as part of their learning experience.
- Teach children how to evaluate internet information and to understand and to take care of their own safety and security.

There are many benefits of the internet to learning:

- Access to world-wide educational resources
- Collaboration and communication between children
- Access to anytime, anywhere learning
- Educational and cultural exchanges to develop global understanding
- Access to experts in many fields for children and staff
- Professional development for staff through access to national developments, educational materials and example of effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of information

With increased use of the internet, protecting and educating children to manage the risk becomes our primary concern. As a school we commit to provide parents with support and information in keeping children safe online.

2. How Fir Tree Promotes E-Safety

2.1 Children

The school has a clear 'Acceptable Use Agreement for Children' which is developed and agreed with the children. This agreement forms the code of conduct. To support appropriate access to the internet and use of electronic communications, we ensure that:

- The E-safety Policy is shared with the children and parents are encouraged to discuss and emphasise the policy for home use
- The E-safety agreement is clearly visible in all classrooms
- Children are informed and are aware that internet use is monitored
- E-safety is delivered to raise the awareness and importance of safe and responsible use of the internet and other electronic communication tools. This is delivered in the classroom through Computing skills lessons and PSHE sessions, and beyond the classroom through structured annual training and specially focused assemblies. E-safety messages are reinforced each time internet access or ICT usage is given

2.2 Staff

As standard practice we ensure that:

- All staff are given the School E-safety Policy and its application and importance explained
- Staff are asked to read and sign the 'Acceptable Use Agreement for Staff'
- Staff are fully aware that internet traffic can and will be monitored and traced to the individual user. Discretion and professional conduct is essential

- The E-safety & Acceptable Use Agreement are a core part of the induction programme for all new staff
- Training for teaching and non-teaching staff in, safe and responsible internet use and on the school E-safety Policy, is provided regularly. Refer to the Code of Conduct for staff on the use of Facebook. Classroom practice is monitored to ensure effective compliance

2.3 Parents

Internet use in the home is increasing rapidly. Parents need to be aware of the dangers and ensure all technological equipment used in the home has the required and appropriate level of age appropriateness and software protection. As a school, we recognise the importance of striking a careful balance between informing and alarming parents. Our policy is to:

- Draw parents' attention to E-safety resources in particular the school's E-safety Policy, relevant articles and resources from trusted sources, and online reporting procedures in newsletters and on the school website
- Handle internet issues sensitively, to inform parents without alarm
- Encourage a partnership approach with parents where careful and informed practice can be supported in and out of school. This includes professionally delivered parent E-safety information sessions that build awareness of benefits and risks, and offer independent advice and best practice suggestions for safe home Internet and e-communications use. In addition to this, useful links are included in the parents section on the school website

2.4 School Governing Body

All Governors of the school are expected to understand, uphold and ensure E-safety best practice for staff and children. As internet and communication access broadens, so governors must ensure that the school keeps pace in its policies and procedures and can effectively protect, educate and respond. To support this, we ensure:

- E-safety and ICT/Computing is part of our School Development Plan
- All Governors receive professionally delivered E-safety training and are clear as to their role in due diligence.
- E-safety is part of the Community and Wellbeing Committee and the members of this committee ensure the effective practice of E-safety is delivered and reviewed regularly
- Governors receive a termly E-safety report outlining implemented practices and any reported incidents each term.

3. How Fir Tree protects against Cyber Bullying and Grooming

As a school we each have a responsibility to ensure our children are kept safe and they understand what cyber bullying and grooming are and know how to protect themselves and report incidents.

3.1 Cyber Bullying

Online bullying and harassment via instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on children both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and un-intended involvement an increased risk.

Fir Tree Junior School has a range of strategies and policies to prevent online bullying, these include:

- No access to public chat-rooms, instant messaging services and bulletin boards.
- Children are taught how to use the internet safely and responsibly and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how

to handle concerns and report incidents) is given as part of an annual Anti-bullying Week and Safer Internet Day.

- Children are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff.
- Children are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our Behaviour and Discipline Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

3.2 Grooming

Grooming is a word used to describe how people gain the trust of children - and possibly their families - with the intention of potentially harming them. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect children against this risk. These include:

- No access to public chat-rooms, instant messaging services and bulletin boards. Children do not have access to their mobile phones during the school day.
- All online access and children generated content in school is monitored and password protected
- Children are taught how to behave responsibly online and the rules in protecting personal information
- Children, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe online

4. Measures and controls to enable responsible internet access and usage

These are outlined below:

4.1 Authorising Internet Use

Children are expected to complete the E-Safety Code of Conduct and are authorised to access the internet as a group or independently, depending on the activity. Internet usage is under the supervision of the teachers and teaching assistants. All staff read and sign the 'Staff Acceptable Use Policy' and parents are requested to share the 'Children's Acceptable Use Policy' with their children.

4.2 Managing Filtering

Our policy is that internet access must be appropriate for all members of the school community. Our ICT systems are managed by Turn It On, a company based in Witney. The procedures for ongoing management and review are:

- The school will work with Turn It On to ensure that systems are reviewed and any improvements needed are implemented
- If staff or children discover unsuitable sites, the URL must be reported to the School Business Manager, who will then report this to Turn It On and ensure that the URL is blocked.
- Any material that the school believes to be illegal must be reported to appropriate agencies (IWF or CEOP)

4.3 Managing E-mail and Communications

All staff are given a secure school e-mail address. The creation of these accounts is the responsibility of the School Business Manager. Should any staff need to contact parents directly then they should

use either the school telephone, their school e-mail, or communication should be passed through to the school office. All personal contact details for staff members will remain private.

In order to enable responsible and safe e-mail use with the children, the following measures are in place:

- Children are taught how to use emails safely and responsibly using the school email system
- Children are taught how to use e-mail during computing skills lessons and educated in the risks and how best to manage them
- The school reserves the right to monitor user's e-mail accounts provided by the school.
- Outside school children are advised not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without parental knowledge

4.4 Password Protection

The children use a password protected 'group' logon to access the school network. The username and password is arranged by the School Business Manager for each class. As part of computing lessons and E-safety teaching, children are taught about the importance of keeping their personal details, including passwords, private.

4.5 Managing Published Content and Images

Our school website celebrates pupils' work, promotes the school, publishes resources and acts as a communication tool. Publication of information on the school website is carefully considered from a personal and school security viewpoint.

Contact details available on the website are school address, e-mail and telephone number. Staff or pupils' personal information is not published and all images used will comply with the conditions below:

- Children's names are published as their first name only
- Staff are referred to by their title and surname
- Any images of children must **not** be labelled with their names.
- Children will only be shown in photos where they are suitably dressed.
- Completed consent forms from parents or carers must be obtained before images of pupils are electronically published. A master list is available and updated by the school office staff.
- While images may be taken by parents, it is requested that they are not shared in the public domain.
- All digital images are securely stored and disposed of in accordance with the Data Protection Act.

4.6 Managing Information Services

Fir Tree Junior School is committed to take due care in regard to managing the provision of Information Services to support secure and appropriate access. The measures outlined in this Policy include:

- Network servers are kept securely in a locked room
- The security of the school information system is reviewed regularly
- The school reserves the right to monitor user areas and equipment provided by the school
- Sophos anti-virus software updates automatically every hour. Staff are also encouraged to install Sophos or any other secure protection at home to increase security
- The school uses Internet firewall and filters provided by Turn It On
- For fire safety network server backups of user data are taken daily and stored remotely using online servers.

4.7 Social Networking and Personal Publishing

Direct access to social networking sites is blocked in school. We recognise that children need guidance and support in knowing how to stay safe online whether in school or at home. Social networking sites have an age limit and it is the responsibility of parents to respect this and to ensure their children are complying with the regulations.

Children need to understand the dangers of uploading personal information and the practical impossibility of removing it. They need to be taught the reasons for caution in publishing personal information and photographs on the internet and in particular on social networking sites. Our E-safety Policy aims to provide guidance and on keeping safe within social networking and personal publishing.

- Children are advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended,
- Children are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff must ensure their profiles on social networking sites are private and not to add present or past pupils as friends.

We very much acknowledge that we cannot act in isolation and parent's co-operation in supporting these steps is greatly appreciated.

4.8 E-Safety Complaints

In the event of a complaint, parents need to discuss their concerns with their child's teacher in the first instance and if not satisfied then they need to see the Headteacher. If the matter is not resolved then the parent will be referred to the school's Complaints policy which is available on the school website or a copy can be obtained from the school office.

Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

4.9 Risk Assessments

In-line with commitments made within this policy, the school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never appear on a school computer. It is the responsibility of the school and staff to ensure our e-safety procedures are followed. All internet access at Fir Tree Junior School is protected under the filtering system set up by the company Turn It On. As part of our e safety procedures, children are taught to understand the risks of using the internet and how best to manage those risks. The Headteacher will ensure that the E-safety policy is implemented and compliance with the Policy monitored.

5. Using the different technologies available

In addition to computers and tablet devices commonly used to access the internet or enable communications, this policy outlines clear guidelines as they apply to other known and used technologies:

- Video conferencing
- Mobile phones
- Online Games

5.1 Video conferencing

We use Microsoft Teams and this will be used for online teaching, homework, meetings with parents and external professionals. Where using Teams may not be possible, Zoom will be used and the relevant safety measures will be adhered to. The practices below aim to ensure that we apply our e-safety commitments to video conferencing:

- When used in the school, video conferencing must be switched off when not in use and not set to auto answer
- Video conferencing contact information will not be put on the school website
- Video conferencing will be supervised by a teacher at all times and the appropriate checks need to be completed before the conferencing begins. This will include; the context of the call agreed; the subject and questions are clear and it must be agreed that any recordings are not to be uploaded on any social networking site.

5.2 Mobile phones

Children are not allowed to have personal mobile phones or other similar devices to use during the school day. Children in year 5 and 6 may bring in their phones if they walk to and from school alone. Parents will be asked to give their permission for this. Any child with parental permission may bring in their phone and will hand it to their class teacher for safe keeping in the secure cabinet in the teacher's cupboard. However, in acknowledgement of the growing use, children will be taught about the benefits and risks, the legal and moral implications of posting photos and personal information from mobile phones to public websites, and how the data protection and privacy laws apply.

5.3 Online Games

Online games can be a helpful and engaging way of developing learning through play with a range of educational content presented through games to support literacy, maths, problem solving, strategy or coding. Controlled use may be supported within the classroom but always through screened individual log-in programs or via teacher-led activity where fit for use and appropriate access settings have been pre-assessed.

We recognise that gaming plays a key part in recreational play in the home setting or when with friends. Best practice guidance can be found in the 'Microsoft Policymaker Guide Online safety'.

We have outlined some best practice guidance which will help to support and keep children safe when using online games outside school:

- Adhere to the age guidance ratings of all games. They are there for a good reason in keeping children safe.
- Select games from only reputable sites. This will help reduce the risk of downloading viruses or sharing data in an unprotected way. Review the game's terms of play to find out how the game service monitors players and responds to abuse and read the site's privacy policy to learn how it will use and protect children's information.
- Play online games only when you have effective and updated antivirus software and firewall running.
- Play only with authorised versions of games which you have purchased from the correct sources and for which you have a licence. Verify the authenticity and security of downloaded files and new software by buying from reputable sources.
- Be aware of the online games where the players communicate. These are unfiltered, unmoderated discussions and can pose a variety of potential risks for children.
- Choose a user name and password with your child that does not reveal personal information. Similarly, if the game includes the ability to create a personal profile, or where contact can be made by other players make sure that no personal information is given away.

E-Safety Policy

- Read the manufacturer or hosting company's terms and conditions to make sure there will not be any immediate or future hidden charges.
- Set guidelines and ground rules for your children when playing online. This could include time limitations, parent entered passwords or game play only in communal areas.
- When disposing of your gaming device either by selling, scrapping, giving away or donating, ensure all of your personal information and your account details have been deleted.

The contents of this policy are regularly reviewed and updated in light of the on-going changes to modern technologies. These will be examined for educational benefit and a risk assessment will be carried out before these can be used in school.

5.4 Behaviours & Sanctions

A critical part of our E-safety Policy which applies across all technologies are the behaviours we seek to embed and the sanctions children or staff may face if their actions put their or others E-safety at risk

Online Behaviours

Personal Information is Personal

Never give out personal details such as name, address, date of birth. School user names and passwords should not contain personal information

Treat others online as you do in the real world

Online bullying and harassment are potential problems that can have a serious effect. Causing upset or harm online will follow the same sanctions as outlined in our Behaviour and Discipline policy

Strangers Online are still Strangers

Friends are people we know and see regularly as part of our everyday lives. Online 'friends' are strangers and invitations to meet them should be reported

Evaluate what you see and do

Evaluate everything you read, and refine your own publishing when using search engines

What to do if something isn't right

If you know or feel something isn't right, speak to, or contact an adult immediately

Sanctions

The school will take immediate action if staff or children were to put themselves or others at risk. The school will follow the appropriate policy guidance

Teachers guide children to appropriate websites, or teach search skills. Information received via the Internet, e-mail, or text message requires good information handling skills. Our approach is to offer children a few good sites as this is often more effective than an internet search. Respect for copyright and intellectual property rights, and the correct use of published material are taught.

Children need to learn to evaluate everything they read and to refine their own publishing and communications with others.

- The school internet access is designed expressly for children to use and includes filtering appropriate to the age of the children.
- Children are taught what internet use is acceptable and what is not and are given clear objectives for internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide children in online activities that support the learning outcomes planned
- ICT skills lessons are used to educate children in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. This is reinforced by teachers when using the internet within their classroom.
- The school ensures that copying and subsequent use of the internet derived materials by staff and children complies with copyright law.
- Children are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Anti- Cyberbullying Policy

We aim to ensure that children are safe and feel safe from bullying and harassment. Our school is committed to teaching children the knowledge and skills to be able to use ICT effectively, safely and responsibly.

Cyber bullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

Aims of this Policy

- To ensure that, staff, children and parents understand what cyber bullying is and how it can be combated
- To ensure that practices and procedures are agreed to prevent incidents of cyber bullying
- To ensure that reported incidents of cyber bullying are dealt with effectively and quickly.

Understanding Cyber bullying

- Cyber bullying is the use of ICT (usually a mobile phone and or the internet) to abuse another person.
- It can take place anywhere and involve many people.
- Anybody can be targeted including children and school staff
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication of private information or images etc.

Procedures to Prevent Cyber bullying

- Staff, children, parents and governors to be made aware of issues surrounding cyber bullying
- Children and parents will be urged to report all incidents of cyber bullying to the school
- Staff CPD will assist in learning about current technologies
- Children will be involved in developing and communicating this policy
- Children will learn about cyber bullying through PSHE, assemblies, Safer Internet Day, Anti-bullying Week activities and other curriculum projects
- Parents will be provided with information and advice on how to combat cyber bullying
- Parents will be expected to discuss the meaning of the Acceptable Use Agreement with their child and sign it
- Children, parents and staff will be involved in reviewing and revising this policy and school procedure
- All reports of cyber bullying will be investigated, recorded and dealt with accordingly
- The Local Authority can provide support and assistance in dealing with incidents of cyber bullying and can be contacted by staff and parents. The police may be contacted in cases of actual or suspected illegal content.

Appendices

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act 1998 and in line with the school's Data Protection policy

The Data Protection Act 1998 ('the Act') gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).

The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be; processed fairly and lawfully, processed for specified purposes, adequate, relevant and not excessive, accurate and up-to-date, held no longer than is necessary, processed in line with individuals' rights, kept secure and transferred only to other countries with suitable security measures.

Acceptable Use Agreement for Staff

The computer system is owned by the school, and may be used by staff to further their education and enhance their professional activities including teaching, research, administration and management. The school's E-safety Policy has been drawn up to protect all parties – the staff, the children and the school. To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to accept this code of conduct as part of their duties and responsibilities as a member of staff of Fir Tree Junior School. Staff should consult the school's E-safety Policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my network area and internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report an incident of concern regarding children's safety to the school's Designated Safeguarding Lead.
- I will ensure that any electronic communications with children are compatible with my professional role.
- I will promote E-safety with the children in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not access any social media sites, this includes Facebook during a school day whether I am in school or at home during the school day.
- The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Acceptable Use Agreement

Name:

Signed:

Date:

Acceptable Use Agreement for Children Code of Conduct

The school has computers, laptops and iPads with access to the internet to support our learning. This agreement will help keep us safe and help us be fair to others.

Using the Computers

- I will only access the computer system with the login and password I have been given
- I will not access other people's files
- I will not bring in memory sticks, CDs or DVDs from outside school and try to use them on the school computers without permission from my teacher

Using Mobile Technology

- I will only use the IT equipment when I have been given permission by my teacher
- I will use the IT equipment responsibly and make sure I return it to the designated station after I have used it
- I will only use apps that I have been given permission to use by my teacher
- I will only take photographs or film children or adults with their permission; only using school equipment
- If I bring mobile technology from home I will hand it to my teacher to put in the class cupboard – my mobile may only be used outside of school (Year 5/6 only)
- I will inform my teacher of any inappropriate messaging from friends on mobile phone messages or chats

Using the Internet

- I will ask permission from a teacher before using the internet
- I will report any inappropriate material to my teacher immediately because this will help protect other children and me
- I understand that the school may check my computer files and may monitor the internet sites I visit
- I will not complete and send online forms without permission from my teacher
- I will not give my full name, my home address or telephone number when using the internet

Using E Mail and Teams Online

- I will only use email with a school account and only use it for school work
- I will only e-mail people my teacher has approved
- I will not give my full name, my home address or telephone number or arrange to meet someone outside school hours
- I will not use email to create group contacts with friends or respond to group contacts; I will inform my teacher if this happens
- I will not create any meetings on Teams and will only attend meetings created by my teacher
- I will use Teams online for Homework and online learning when my teacher sets work

I agree to this code of conduct. If I break this agreement I could lose the privilege of using the internet in school

Child's Name:

Class:

Parent's Name:

Date:

E-Safety Contacts and References

Childnet International

<http://www.childnet.com/resources>

Childline

<http://www.childline.org.uk>

Think U Know (links to CEOP)

www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre

www.ceop.gov.uk

Stop it now (child sexual abuse prevention campaign, for all adults)

www.stopitnow.org.uk

Parents Protect

www.parentsprotect.co.uk

E-Safety self-review tools provided by South West Grid for Learning

www.360safe.org.uk for schools and www.onlinecompass.org.uk for youth settings

Securus (Company supplying software to protect pupils from cyberbullying in schools)

www.securus-software.com

Internet Watch Foundation (IWF)

www.iwf.org.uk was set up by the UK internet industry to provide the UK internet 'Hotline' for the public to report potentially illegal online content.

CBBC Stay Safe

www.bbc.co.uk/cbbc/topics/stay-safe

Web Cam fact sheet

<http://www.thinkuknow.co.uk/Documents/Webcam%20fact%20sheet%202.pdf>

Kidsmart

<http://www.kidsmart.org.uk/>

NSPCC

<http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm>

Report it:

Thames Valley Police – for suspected criminal activity

<http://www.thamesvalley.police.uk/reptcr/reptcr-repform.htm>

Oxfordshire County Council website – for child safeguarding concern

<http://www.oxfordshire.gov.uk/cms/public-site/child-social-care>

CEOP – report a child in danger of abuse. Children can self-report.

<http://www.ceop.police.uk/safety-centre/>

Virtual Global Taskforce – Report Abuse

<http://www.virtualglobaltaskforce.com/>

Internet Watch Foundation – report child sexual abuse content

<http://www.iwf.org.uk/> Professionals Online Safety Helpline_0844 3814772

E-Safety Check

- Only use the internet when there is a teacher or other adult present to supervise or when you have been given specific permission
- Only use the login name and password provided by your teacher.
- Never give out your address, phone number or arrange to meet someone over the internet
- Never send out photos of yourself to anyone without your parent's permission
- All e-mails, messages in forums and text messages should be polite, appropriate and sensible. Do not send any e-mail or text message which could be hurtful towards the person or any other person
- If you receive a rude or offensive message you must report it to a teacher immediately. Do not pass on rude or offensive messages. What may seem funny to you may not be funny to someone else
- If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher
- The school has the right to check your computer files and monitor the internet sites you visit
- Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate
- You and your parents should have signed the school 'Acceptable Use Agreement'. You will be breaking that Agreement if you deliberately break these rules. This could result in you losing your internet access at school.
- E-Safety applies in school and at home

Copyright Release & Digital Video Information

Copyright Release

The school may produce printed publications and/or a school web site which may include examples of pupil's work and/or photographs of pupils. No child's work will ever be used without his/her permission and we take the issue of child safety very seriously which includes the use of images of pupils. Including images of pupils in school publications and on the school website can be highly motivating for the pupils involved, and provides a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents let us know their preferences regarding the use of their children's work and/or photographs and video by completing an online poll.

Digital Video

Digital video is an exciting medium which can motivate and inspire pupils. Research has shown that using digital video in education can help encourage creativity, motivate and enthuse pupils, and improve communication and team-working skills. We use digital video as part of our learning and teaching, and for the recording of school productions and events.

We ask that parents give written consent to their child taking part in the production of digital video, and/or appearing in films.

Although the risks of using digital video in education are minimal, schools have a duty of care towards pupils. This means that pupils will remain unidentifiable, reducing the risk of inappropriate contact, if images or examples of their work (including digital video) are used on the school website.

Parent/Carer Permission and Copyright Release

I consent to photographs and digital images of my child, appearing in printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as the schools newsletter, school prospectus and occasionally in the local papers, as part of the promotional activities of the school.

I further consent to examples of my child's work being published on the school website or in other media, subject to strict confidentiality of personal information as compliant with the Data Protection Act.

Parent/Carer Name, Signature and Date

Digital Video

I consent to my child taking part in Fir Tree Junior School projects using digital video. I consent to my child taking part in the production of digital videos and appearing in films. I understand that films may be made available on the school website or used in other school promotional activities.

Child's Name:

Class:

Parent's Name:

Date:



Fir Tree Junior School
E Safety Incident Recording Form

Name					
Date					
Class					
Type of Incident Provide detail of the incident; where it happened and the equipment used at the time					
Child/Children involved					
Contact with other agencies needed					
Actions taken					
Signed		Print name		Date	
Headteacher's use only Actions					

Infrastructure/Network

E-Safety Lead:	Nathan Wilcox (Computing Subject Leader) Annette Yener (School Business Manager)
DSL	Nilofer Khan (Headteacher)
E-Safety Governors	Anna Perryman, Tom Gould, Steve Hutton (Community and Wellbeing Committee)
External IT support	Turn It On

Responding to incidents of misuse – flow chart



