THE ORATORY
PREPARATORY SCHOOL

ONLINE SAFETY POLICY (e-Safety) including Pupil Acceptable Use Policy

September 2019

1. INTRODUCTION

The Oratory Preparatory School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibly and that pupils, staff and parents use it appropriately and practice good online safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours.

As part of our commitment to learning and achievement we at The Oratory Preparatory School want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen we have taken a whole school approach to E-safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

1.1 The Oratory Preparatory School as part of this policy holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.

1.2 The Oratory Preparatory School is committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated in dangers that exist so that they can take an active part in safeguarding children from them.

1.3 The nominated senior person for the implementation of the School's e-Safety policy is The Designated Safeguarding Lead, Mrs Gill Smith.

The E-Safety policy should be read in conjunction with the following policies for further clarity:

- Safeguarding and Child Protection,
- Anti-Bullying
- Behaviour
- Staff Code of Conduct and pupils Acceptable Use Policy
- SRE and PSHE
- Data Protection/GDPR
- Social Media and EYFS Telephone calls/mobile phones/camera/video recorder usage policy.

It is also informed by DfE guidance, including Keeping Children Safe in Education 2019 (KCSIE).

2. SCOPE OF POLICY

2.1 The policy applies to:

- ALL pupils;
- ALL teaching and support staff (including peripatetic), school governors and volunteers;
- ALL aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 The Oratory Preparatory School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the internet and digital technologies;
- education that is aimed at ensuring safe use of internet and digital technologies;
- a reporting procedure for abuse and misuse.

3. ROLES AND RESPONSIBILITIES

3.1 The Headmaster and Senior Management Team (SMT)

The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety co-ordinators. Any complaint about staff misuse must be referred to the online safety coordinators at the school or, in the case of a serious complaint, to the Headmaster.

- Ensure access to induction and training in online safety practices for all users.
- Ensure all staff receive regular, up to date training.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SMT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.

- Work in partnership with the DfE, the Internet Service Provider and school ICT Manager to ensure systems to protect students are-appropriate and managed correctly.
- Ensure the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.

3.2 The E-Safety Coordinator/s

The persons responsible for e-safety at the Oratory Preparatory School are the Head of ICT (see development plan), the Designated Safeguarding Lead and the Head of Girls with support from the ICT Technical Team and ICT Support for educational platforms.

The role of the e-safety coordinators:

- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policy.
- Ensures all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Have regular meetings to review issues and ensure updates are noted, implemented and shared.
- Arrange and provide training and advice for staff.
- Work in partnership with the DfE, Local Authority and Internet Service Provider and school ICT manager to ensure systems to protect students are age-appropriate and managed correctly.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering control logs.
- Reports regularly to the Senior Management Team.

3.3 The Technical Staff

It is the responsibility of the Oratory Preparatory School to ensure that the ICT department technical staff carries out all the e-safety measures. It is also important that the technical staff are fully aware of the schools' e-safety policy and procedures.

The technical staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- that they 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,
- that the use of the network / internet / Virtual Learning Environment / remote access / in order that any misuse / attempted misuse can be reported to the

Designated Safeguarding Lead, Headmaster or E-Safety Coordinators for investigation / action / sanction

- that monitoring software / systems (including online testing)are implemented and updated as agreed in school policies

4. Communicating School Policy

This policy is available on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and online safety guidelines, are displayed in specific classrooms in the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

5. EDUCATION AND TRAINING - Pupils

The Oratory Preparatory School recognises that the internet and other digital technologies can transform learning and we want to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the internet and other digital technologies safely.

To this end, The Oratory Preparatory School will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum. This is provided as part of Computing, RSE, PSHE, assemblies and other relevant subjects/pastoral lessons.

- Educate pupils to acknowledge the source of information used and to respect copyright using materials accessed on the internet.

- Educate pupils to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Use age-appropriate tools to search for information online. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can

temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

6. EDUCATION AND TRAINING – teaching and support staff

The Oratory Preparatory ensures ALL staff have an up to date awareness of e-safety matters and of the current school's e-safety policy and practices.

The E-Safety Coordinators will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.

- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- The E-Safety Coordinators and ICT Technical Support team will provide advice / guidance / training to individuals as required.
- The staff will embed e-safety issues in all aspects of the curriculum and other activities when/where appropriate.
- The staff will monitor the use of digital technologies, mobile devices, cameras, iPads etc, in lessons and during other school activities (where allowed) and implement the current and relevant policies with regard to these devices.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites, then the URL will be reported to the *school technical support team.* Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

The Designated Safeguarding Lead will be trained in e-safety issues and be aware of the potential serious safeguarding issues to arise from:

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

7. EDUCATION AND TRAINING – Parents/Carers

We recognise parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the 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 Oratory Preparatory School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site and E Safety Information Packs.
- Parents / Carers evenings / sessions and workshops where parents can share their experiences and worries and be guided on how best to supervise and educate their children about e-safety.
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

(see Appendix II for further links / resources)

8. POLICIES AND PROCEDURES

We at The Oratory Preparatory School understand that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist with The Oratory Preparatory School are aimed at providing a balance between exploring the educational potential of new technologies and providing safeguards to pupils.

Managing Information Systems – please refer to our Data Protection Policy which can be found on our website.

8.1 Use of internet facilities, mobile and digital technologies

The Oratory Preparatory School will seek to ensure that Internet, mobile and digital technologies are used sensitively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

The Oratory Preparatory School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Indecent images of children

[1] For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts

8.2 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required.

8.3 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

8.4 <u>In addition, users may not:</u>

- Use the Association provider's facilities for running a private business;
- Enter into any personal transaction that involves the Association
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of the associations;
- Reveal or publicize confidential or proprietary information, which includes but is not limited to:
  - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorized access to facilities or services accessible via the associations
- Undertake activities with any of the following characteristics:

- wasting staff effort or networked resources, including time on end systems accessible via the associations network and the effort of staff involved in support of those systems;
- corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users;
- using the associations network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- continuing to use an item of networking software or hardware after the associations has requested that use cease because it is causing disruption to the correct functioning of the associations;
- Use mobile technologies 3G, 4G, 5G or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

9. EMAILS

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

9.1 School Email Accounts and Appropriate Use

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

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are always representing the school and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior management team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use school-approved email accounts
- Social emailing is not permitted.

- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

9.2 Reporting Abuse

Anyone who becomes aware of an e-safety incident should **record** the facts and information on the school's safeguarding concern form. This should be passed on to the Designated Safeguarding Lead.

9.2.1 If a child or adult receives an abusive email or accidentally accesses a website that contains abusive material.

- Report to the Designated Safeguarding Lead

9.2.2 If a member of staff is concerned that a child is at risk of **significant harm**.

- A telephone referral must be made as soon as possible to the LADO.
- In an emergency, call 999 to contact the Oxfordshire Police.

9.2.3 If your concern is about cyberbullying, commercial exploitation, inappropriate or illegal content of a website, but you do not think a child or young person is at risk of significant harm.

- Report to the Designated Safeguarding Lead

10. Mobile Phones and Personal Device

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly.

The Oratory Preparatory School has a strict 'NO MOBILE PHONE' policy for pupils (with the exception of boarders who have restricted and monitored use in the boarding house).

In additions we:

- The School will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy.**
- A member of staff can confiscate mobile phones which are brought into the school without permission (including the boarding house), and a member of the senior membership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- If staff wish to use personal mobile phones in class as part of a learning project, they must get permission from the Headmaster and Designated Safeguarding Lead.

For further information on use of mobile phones and devices please refer to the following polices:

- Social Media and EYFS Telephone calls/mobile phones/camera/video recorder usage policy.
- Staff Employment Manual
- Staff Code of Conduct and Acceptable Use Policy

11. Published Content and the School Website – Please refer to OSA Social Media Policy Jan 2019

12. Complaints of Misuse of Photographs or Videos – Please refer to our Complaints Policy.

13. MONITORING

13.1 Monitoring the safe use of the internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. The Oratory Preparatory School recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

13.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, The Oratory Preparatory School will audit the use of the Internet in order to ensure compliance with this policy. The school will also work with its Internet service provider to further ensure compliance.

13.3 The Oratory Preparatory School will ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm through use of the Internet.

APPENDICES OF THE E-SAFETY POLICY

APPENDIX I

List of authorised persons who have various responsibilities for E-safety;

Name	Responsibility	Contact Number
Mrs Gill Smith	Designated Safeguarding Lead	01189 766919 (Office Number – office hours) 07872 562667 Mobile Number 01189 844511 (School Number and out of office hours) g.smith@oratoryprep.co.uk
Mr Chris Sexon	Deputy Safeguarding Lead	01189 844511 (School Number and out of office hours) c.sexon@oratoryprep.co.uk
Mr Rob Stewart	Headmaster	01189 844511 (School Number and out of office hours) 07789304813 Mobile Number headmaster@oratoryprep.co.uk
Mrs Kate Oakley	Deputy Safeguarding Lead Head of Pre-Prep	01189 766903 (School Number and out of office hours) k.oakley@oratoryprep.co.uk
Mrs Melanie Williams	Head of Girls	01189 844511 (School Number and out of office hours) m.williams@oratoryprep.co.uk
Ronan O'Sullivan	Technical Support (Filtering and security)	01491 683555 (Office Number – office hours) r.osullivan@oratory.co.uk or support@oratory.co.uk

APPENDIX II

Useful Contacts and websites – this list is not exhaustive

CONTACTS – for reporting and help
Oxfordshire County Council - https://www.oxfordshire.gov.uk/cms/content/internet-safety-advice

O2 and NSPCC internet safety helpline - http://www.o2.co.uk/help/nspcc

NSPCC - Free helpline for parents to help them keep children safe online **0808 800 5002**.

Thames Valley Police – for suspected criminal activity
http://www.thamesvalley.police.uk/reptcr/reptcr-repform.htm

CEOP – report a child in danger of abuse. Children can self-support.
http://www.ceop.police.uk/safety-centre/

NATIONAL RESOURCES
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

http://www.goffs.herts.sch.uk/information/school_info/esafety.shtml

http://www.parentsprotect.co.uk/what_to_do_if_a_child_tells_about_abuse.htm

http://www.net-aware.org.uk/

http://www.chatdanger.com

https://www.thinkuknow.co.uk/parents/

www.kidsmart.org.uk

Useful websites with advice for teachers/parents/guardians:

Think U Know: **www.thinkuknow.co.uk/parents/**

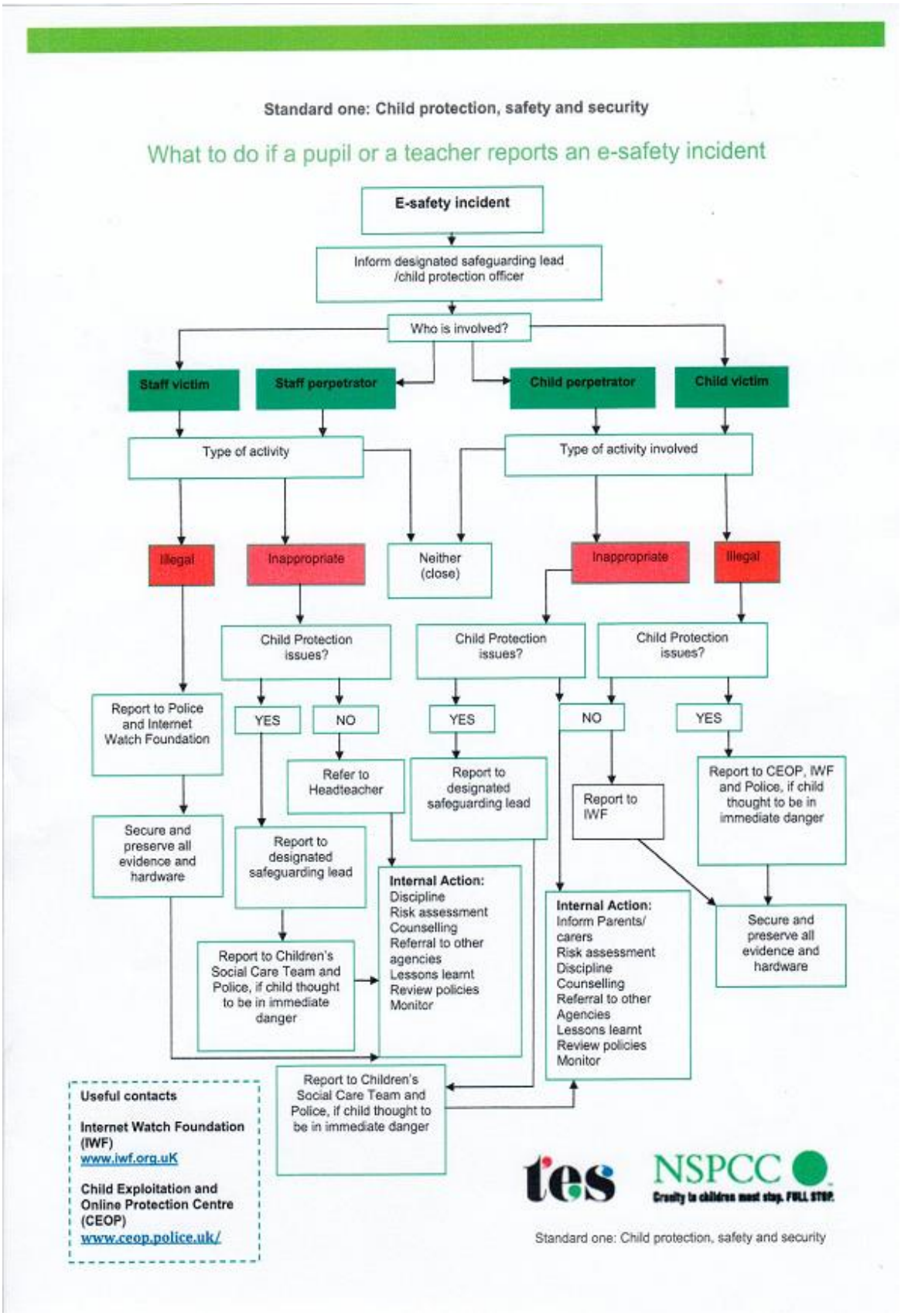
GetNetWise: **www.getnetwise.org/**

Child Exploitation and Online Protection Centre: **www.ceop.gov.uk/**

Chatdanger: **www.chatdanger.com/**

APPENDIX III

What to do if a pupil or teacher reports and e-safety incident



APPENDIX IV

Procedures for responding to careless/deliberate incidents of misuse

All members of the school community will be responsible users of digital technologies, who understand and follow the school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the ***url*** of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the Oratory Preparatory School and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed information form should be retained by the group for evidence and reference purposes.

APPENDIX V

Acceptable Use Policy

Foundation Stage and Key Stage 1

In common with most technologies, internet use presents risks as well as benefits. To ensure responsible use and the safety of pupils, the school's policy is built on the following principles:

- **Responsibility**
  Pupils are encouraged to take responsibility for their safe use of the internet.

- **Education**
  Pupils discuss and learn about acceptable uses of the internet and its possible dangers in ICT and PSE lessons. Pupils know what to do if they come across inappropriate material when using the internet.

- **Technical prevention**
  The school invests in technical solutions, such as firewalls and filters that aim to prevent access to unsuitable material on the internet, although it is accepted that no technical method can be 100 per cent effective.

- **Regulation**
  Fair rules, written for pupils to read and understand, are prominently displayed as a constant reminder of the expectations regarding internet use. These rules are set out below, along with sanctions that may be applied if the rules are not followed.

This is how we stay safe when we use computers:

1. I will ask a teacher or suitable adult if I want to use the computers/tablets.
2. I will only use activities that a teacher or suitable adult has told or allowed me to use.
3. I will take care of the computer and other equipment.
4. I will ask for help form a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
5. I will tell a teacher or suitable adult if I see something that upsets me on the screen.
6. I know that if I break the rules I might not be allowed to use a computer/tablet.

Name of Child: ……..

Parent/Guardian Signature: ……..

Parent/Guardian name (print): ……

APPENDIX VI

Acceptable Use Policy

Key Stage 2 and Key Stage 3

In common with most technologies, internet use presents risks as well as benefits. To ensure responsible use and the safety of pupils, the school's policy is built on the following principles:

- **Responsibility**
  Pupils are encouraged to take responsibility for their safe use of the internet.

- **Education**
  Pupils discuss and learn about acceptable uses of the internet and its possible dangers in ICT and PSE lessons. Pupils know what to do if they come across inappropriate material when using the internet.

- **Technical prevention**
  The school invests in technical solutions, such as firewalls and filters that aim to prevent access to unsuitable material on the internet, although it is accepted that no technical method can be 100 per cent effective.

- **Regulation**
  Fair rules, written for pupils to read and understand, are prominently displayed as a constant reminder of the expectations regarding internet use. These rules are set out below, along with sanctions that may be applied if the rules are not followed.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the systems or devices for on-line gaming, on-line gambling, Internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I understand social media sites are blocked in school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this

agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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 devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school, e.g. communicating with other members of the school, accessing school email, website etc.

Name of Pupil: .....

Year Group/Class: .....

Signed: .....

Date: .....

Parent / Guardian Countersignature: .....

APPENDIX VII

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.