Oaktree E-safety Policy and Procedures

1.0 Introduction

1.1 Oaktree School is aware that the Internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. As such this policy sets out guidelines for the acceptable use of the Internet that will ensure that the pupils of the school can benefit from its use and remain safe. In addition this policy provides all members of the Oaktree network community with guidance to achieve this by helping them to recognise the risks and take action to help children use the internet safely and responsibly.

2.0 Aims

2.1 It is Oaktree Primary School's aim that the educational and social benefits of the Internet should be promoted, but that this should be balanced against the need to safeguard children. To achieve this, we have developed an e-safety strategy and will work in partnership with parents and carers to deliver it.

2.2 Pupils who access the Internet from the school site are required to make safe and responsible choices for actions that take place while using their computers. All children are made aware that all internet activity is logged. Those who access the Internet outside the school are also expected to fulfil all the contractual obligations of the school's e-safety policy.

2.3 Prevent Duty: Our students are especially vulnerable to the risks of radicalisation due to their complex needs and learning difficulties: they are easily led, often over friendly and at times unable to recall conversations or events accurately.

Should staff have any concerns over a student's internet activities which may result in a change in behaviour, language, manner or disposition, or is known to visit radical websites, we have clear procedures for in depth investigations to understand any potential threat or harm which we follow.

2.4 Oaktree Primary School will allow pupils, teachers, other members of the Oaktree network community access to its computers, network services, and the Internet. All pupil activity, when using the network and Internet in school, must be in support of education and/or research and must be appropriate to the educational objectives of the school.

3.0 Benefits

3.1 Use of ICT is so universal that it is of huge benefit to children to learn these skills in order to prepare themselves for the working environment. Access to the Internet will enable staff and pupils to:

- raise educational attainment, by engaging and motivating pupils to learn and so improve their confidence;
- improve pupil's research and writing skills;
- overcome communications barriers, especially helping those with a disability;
- send and receive email;
- engage in projects that involve online reporting to parents;
- enable children to be taught "remotely", for example children who are unable to attend school;
- improve pupil's wellbeing through the social and communications opportunities offered;
- provide access to a wide range of online media for learning and teaching resources;
- exchange personal communication with other Internet users in the UK and across the world;
- publish and display work on the school's website

4.0 Effective Use

4.1 Internet access will be planned to enrich and extend learning activities as an integral aspect of the curriculum. Pupils will:
• be given clear objectives of Internet use;
• be educated in responsible and effective Internet use;
• be supervised appropriately;
• learn to search for and discriminate between valid and inappropriate material;
• learn to copy, save and use material found on the Internet without infringing copyright.

5.0 Safety
Internet access at Oaktree Primary School is filtered by our Internet Service Provider (ISP) a BECTA approved provider. The school prides itself on developing safe and responsible behaviours in all pupils so that each pupil is equipped to make suitable and correct choices when using the internet. However the school will be responsible for any incidents that occur during school time in school. The safe use of the internet at home will remain the parents' responsibility. There will be some provision to ensure that all sections of the school community are kept up to date with current e-safety practices.

This will include:

- The school following the 'Think u know' training safety programme to ensure that training provided is relevant and effective to all sections of its community.
- The signing of a Home School Agreement which includes a statement on internet safety
- The nomination of two e-Safety officers from amongst staff who are known to the children and to whom the children can come if they have any concerns
- An annual meeting for parents to advise them on safe practice

6.0 Personal Security Guidelines
6.1 Pupils should:
• never reveal personal information, either their own or others, such as home addresses, telephone numbers and personal email addresses;
• not use photographs of themselves on their Web pages unless the parent or guardian has given permission to do so;
• never meet people in person that they have contacted on the Internet without parent/guardian permission;
• notify their teacher or e-Safety officers whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable;
• be aware that the author of an Email or Web page may not be the person they claim to be.
- Staff should use their LGfL email account (not their private address) for all school communication

7.0 Managing Email
7.1 Children may receive email directly from known addresses and they may also use their personal email address when replying to known recipients. lgflmail hosts an email system that allows pupils to send emails to others within the school or to approved email addresses externally. Each child receiving Email is encouraged to reply promptly.

8.0 School and Personal Web Pages
8.1 Pupils are encouraged to take an active role in writing Web pages. This often inspires pupils to publish work to a high standard for a wide and varied audience. Web pages can be used to:
• document curricular research;
• be part of an online project;

• promote the school and community;
• publish resources for projects and homework;
• create personal pages detailing interests and displays of work.

9.0 Pupil Responsibility

9.1 Pupils are responsible for appropriate behaviour on the school's network just as they are in the classroom or school playground. It must be remembered that communications on the network are often public in nature.

9.2 General school rules and the Behaviour Policy apply and it is expected that users will comply with the guidelines of this policy.

9.3 Any incidents of cyber bullying should be reported to the e-Safety officers who will record the incident and ensure that the incident is dealt with in line with the school's Behaviour Policy. Incidents should be monitored and the information used to inform the development of anti-bullying practice.

9.4 Pupils are personally responsible for their actions when using school equipment to access computer resources outside the school network.

10.0 Parental Support

10.1 Pupils could potentially have unfiltered, unsupervised Internet access at home. All parents should be aware of the concerns and benefits of Internet use. Parents are therefore welcome to come in to school to work alongside the teacher to experience the Internet first hand. Arrangements for this can be made with the class teacher directly.

11.0 Usage Rules and Guidelines

11.1 Privacy

• Each teacher will ensure that the SMART rules are taught at the beginning of each academic year and revisited again to encourage pupils to make safe and responsible choices when using the internet at all times.
• Photographs of pupils that will appear from time to time on the school's website will not be labelled.
• Teachers and staff may review documents and log files to ensure that pupils are using the system responsibly.

- Security passwords will be used on all devices which contain confidential data on pupil's attainment and well-being. Memory devices will be encrypted for similar protection.

11.2 Software

• Pupils should never download, load or install any software, shareware, or freeware, or load any such software from USB sticks, unless they have permission from their teacher.
• Pupils may not copy other people's work or intrude into other people's files without permission.
• Inappropriate materials or profane, abusive and impolite language should not be used to communicate nor should materials be accessed which are not in line with the rules of school behaviour.
• A good rule to follow is never view, send, or access materials that you would not want your teachers or parents to see. Should pupil encounter such material, they should immediately report it to their teacher.
• Children are only allowed in chat rooms with teacher permission.
• No Internet games may be played during school hours

11.3 Safe teaching Practice

• Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.

• Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the Internet; remarks that are private may go to wider audience and raise questions regarding confidentiality.
• Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.
• When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone.

12.0 Responding to Incidents

12.1 All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-Safety officer and the ICT Leader of Learning.
12.2 All incidents, whether involving pupils or staff, must be recorded by the e-Safety officer on the 'Logging a Concern' form which is kept in the Headteacher's Child Protection Reports file.
12.4 Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action. Incidents involving the head teacher should be reported to the chair of the board of governors.
12.5 The school's e-Safety officer should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-Safety system, and use these to update the e-Safety policy.
12.6 E-Safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection person, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the head teacher.
12.7 Although it is intended that e-Safety strategies and policy should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Enfield can accept liability for material accessed or any consequences of Internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

13.0 Breach of the e-Safety Policy

13.1 The head teacher will decide what sanctions will be applied for breach of the e-Safety policy. The sanctions applied will reflect the seriousness of the breach and will take into account all other relevant factors. Examples of a breach are:
• persistent and/or extreme cyber bullying;
• receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act;
• bringing the schools name into disrepute.

Sanctions could include:
• referral to the head teacher;
• banned use of the internet for a defined period
• removal of device/equipment;
• contact with parents;
• possible exclusion;
• referral to Enfield's e-safety officer.
• referral to community police officer

14.0 Staff Acceptable Internet User Agreement

14.1 All staff complete an Internet User agreement annually as part of our Safeguarding procedures (Appendix 1)

15.0 Logging a Concern form
15.1

• All incidents must be documented on the form as soon as the incident occurs.
• All information pertaining to the incident must be logged in a timely manner as soon as it is reported and investigated with times and dates included.
• It is vital that details are not logged in retrospect as further investigation of an incident may involve external agencies. (Appendix 2)

16.0 Conclusion

16.1 This policy has been written in conjunction with the school's Behaviour and Child Protection Policies.

16.2 This policy describes strategies and procedures that reduce the risks of e-Safety breaches and or data security incidents. Oaktree School will update this policy to reflect new developments as and when needed.

DISSEMINATION OF THE POLICY

The policy will be given to all members of staff and copies will be available for parents.

PROCEDURES FOR MONITORING AND EVALUATION

The head teacher, members of the senior management team and members of the curriculum leadership team, will monitor the policy.

September 2017