Oakfield School

45. E-Safety Policy

To be Reviewed:	September 2017

Ethos

At Oakfield, we believe it is every pupil's right to expect excellent teaching of an enriched and engaging curriculum, in a safe learning environment, which will enable them to reach their full potential so that they become prepared for adult life.

We believe that education is about acquiring good personal and thinking skills, developing communication and ICT skills; it is about becoming creative and reflective. This, we believe, enables students to achieve their full academic potential.

We believe that education is also about developing self-confidence, maturing socially and emotionally and becoming independent, able to make sound lifestyle choices based on enquiry and reasoning.

All our pupils will be treated fairly and with respect.

We believe we should set challenging targets for both staff and pupils, building on strengths and striving for improvements.

To promote high standards in lessons and behaviour, we will have effective systems for reviewing and developing our practice as part of our self evaluation and quality assurance programme.

We aim

1. to create a safe and secure learning environment in which high standards of behaviour and commitment are clearly expressed and realised;
2. to create a culture of high expectations and success for pupils, providing a flexible curriculum that engages and motivates groups of pupils and individuals;
3. to promote a sense of responsible citizenship in our pupils;
4. to build a professional community of teaching and support staff within the school, developing leadership skills and teamwork;
5. to build a capacity for future thinking, problem-solving and planning and distributive leadership;
6. to establish collaborative working with other schools;
7. to support and facilitate inter-agency work as part of a broader community approach to learning;
8. to establish and/or maintain and develop positive working relationships with parents and carers for the benefit of the child and their families.

In all these endeavours we will create a culture of pride in our school and raise its profile in the community and across the city. We will take opportunities to reward and celebrate our successes and will acknowledge and seek ways to improve.

1. Writing and reviewing the e-safety policy

Our e-Safety Policy has been written, following government guidance. It has been agreed by all staff and approved by governors.

- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was written by: R Davies

2. Teaching and learning

Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority and school's ICT support.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents/carers

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator: Leanne Foley or Jayne Oakley (Safeguarding)
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used by staff during lesson time. The sending of abusive or inappropriate text messages is forbidden.
- Children are advised not to bring mobile phones to school, however if they do bring mobile phones to in to school there is an expectation that they will manage the use of their mobile phones appropriately and not access Social Network/Media whilst at school. If inappropriate use is deemed then the pupils will be challenged and this could lead to the phone being confiscated.
- Staff will use the school phone where contact with parents is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Policy Decisions

Authorising Internet access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents and carers will be asked to indicate on the pupil's information record whether they agree to their child/ren using the Internet in school. These records are kept centrally in the school office.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

5. Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety will be included in appropriate PSHE lessons and Tutor Time.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be required to sign a Staff Acceptable Use Agreement/Code of Conduct form

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school handbooks and on the school Web site.

Failure to Comply

- Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff.

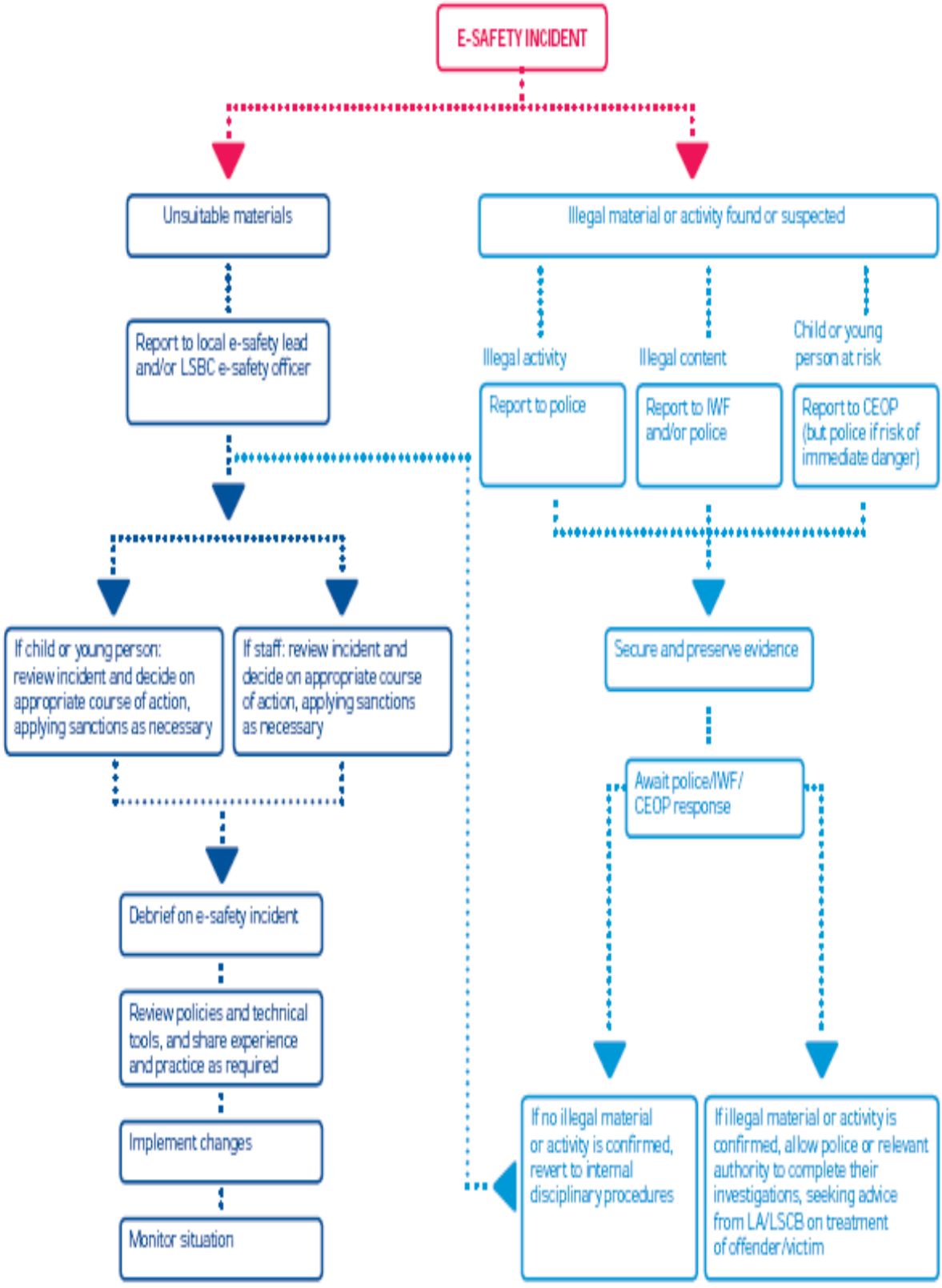
Linked policies

- The E-safety policy should be read in conjunction with the LA approved Facebook policy, as it relates to both staff and pupils.

Appendices

Flowchart for responding to e-safety incidents.
Acceptable use policy for students.
Staff Acceptable Use Agreement / Code of conduct

Flowchart for responding to e-safety incidents



Oakfield School
Acceptable Use Policy for students

I understand that every time I logon to the school network I am agreeing to the Acceptable Use Policy for students as described below.

Using school equipment

- I will respect and look after any school ICT equipment, for example laptops, cameras, keyboards etc. If I use any ICT equipment that is already damaged I will report it to my teacher.
- I will not download or install software on school equipment.

Security and safety

- I will only logon to the school network and internet with my own username and password.
- I will not reveal my passwords to anyone. I am advised to change them regularly.
- I understand that every time I logon to the internet through the school network I am agreeing to their terms and conditions.
- I will not attempt to bypass the school's internet filtering system.
- I will not give out any personal information such as my name, phone number or address on the internet.

Communication

- I will only use my school e-mail address to contact teachers.
- I will make sure that all e-mail communications with students, teachers or others is responsible and sensible.

School purposes

- I will only use the school's ICT for school purposes. This includes the internet and e-mail.
- I will only take images and audio recordings of staff/students with appropriate permission and use them for school purposes. (I understand that parents/carers are required to give their permission for images of their children to be taken and used by the school. I will respect their decision.)

Behaviour

- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

- I will ensure that my online activity, both in school and outside school, will not offend or embarrass my school, the staff or students.

- I will respect the privacy and ownership of others' work on the school network and on-line at all times.

Monitoring

- I know that all my computer and internet use on school equipment is monitored. I know that the monitoring software will record any images, text or keystrokes it considers inappropriate. I know that this information is available to the Leadership Team.

Accessing my school desktop from home

- I understand that the above statements still apply if I use the 'cc4anywhere' software from home to access my school desktop.

I understand that the Acceptable Use Policy is designed to help keep every member of the school community safe.

I understand that if I do not follow these rules, school sanctions will be applied and my parents/carers may be contacted.

Staff Acceptable Use Policy

Data protection

- I understand that I **must not** disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- I understand that I **must not** allow any student to use my personal login to any of the ICT systems for ANY reason.
- I understand that pupils **must not** be allowed to use STAFF PCs
- I understand that I must take every reasonable precaution to secure any data or equipment removed from the school premises.
- I understand that equipment taken off site will be my personal responsibility and I am advised to check that its loss or damage is covered by my personal insurance.
- I understand that the School can and will monitor any data on the network, even if the device is NOT on school site, to ensure policy compliance, and to aid in resolving networking issues.

Use at Home

- All school equipment can be monitored through Securus even if the equipment is not on the school site.
- The school expects staff to use equipment in an appropriate manner and for appropriate uses even when outside the school site.
- Employees will maintain conduct of the highest standard such that public confidence in their integrity is sustained. – Terms and Conditions of Employment, Para 2 (2.1)

Student protection

- I am aware of all guidelines to conceal student identities when publishing to the public domain.
- I understand that students must be supervised at all times when in an ICT suite or on computer equipment.
- When arranging use of ICT facilities I will ensure that a staff member is able to monitor pupils at all times.
- I have read and understand my role regarding acceptable use and my role in enforcing it.
- I will escalate non compliance by students in accordance with school policy.

Reporting incidents

- I will inform a member of the network management staff in writing/verbally immediately of any websites accessible from within school I feel are unsuitable in any way for student consumption.
- I understand my part in maintaining the accuracy of the filtering system.
- I will inform a member of the network management staff in writing/verbally immediately of abuse of any ICT system(s) - software and hardware - providing the location and names where possible.

- I will inform a member of the network management staff in writing immediately of any inappropriate content suspected to be on the ICT system(s). This may be contained in email, documents, pictures etc.
- I will report any breaches, or attempted breaches, in security to a member of the network management staff in verbal/writing immediately.

Software, hardware, copyright and licensing

- I will not attempt to install any software or hardware.
- Before purchasing any hardware or software I will consult a member of the network management staff to check compatibility, license compliance and discuss any other implications that the purchase may have.
- I will respect copyright and make sure I do not use any information breaching copyright law.
- Under no circumstances must any software from potentially illegal sources be installed.

Internet and Social websites

The school recognises the massive educational potential of Web 2.0 Technologies including and not limited to Social Networking, Blogging, Micro Blogging and media sharing sites.

The school encourages staff to use these technologies but for research purposes and the sharing of good practice. In using such technologies and platforms staff should adhere to the following guide:

- Staff should not mention the school in a negative manner. This includes all stake holder's pupils, colleagues, and parents.

- Staff should refrain from commenting on incidents that occur within the school directly.

It is expected that, in all every area's of communication, staff will maintain proper professional distance from pupils currently at school: this must include rejecting requests by them to be added as friends, on all forms of social websites and taking all the measures available within the platforms to deny them access to profiles, personal information and online communications, keeping this strictly to whoever is on your allowed friends lists.
It is strongly advised you do not have past pupils on your friends / contact lists (please seek advise from a member of the senior leadership team should you need further advice)
All forms of social website access within school is currently denied.

I agree to abide by the above statements
……

Name

Date

Department

This Policy was reviewed October 2015.

Signed: **…….**

Mr Lee Morfitt (Chair of Governors)