POLICIES/ REGELVERK

APPENDIX TO CODE OF CONDUCT

**E-Safety Policy**

| | |
|---|---|
| Prepared by: | Head Teacher |
| Approved by: | The Governors |
| Last updated: | 04.10.2018 |
| To be reviewed: | 01.10.2019 |
| Responsible for Online Safety: and ICT-coordinator | Head Teacher |

Children are quite often vulnerable to risks on the Internet. The Norwegian School in London is aware of this and is therefore working on this matter continuously both in staff training and directly with the children. One of the basic skills in The Norwegian curriculum is Digital Skills. The development of digital skills means to learn to use digital tools, digital medias and digital resources. Further, the use of digital tools allows children to learn different skills and express their own competence. There is also an additional skill of judgement and independence when using digital tools.

Referring to the Department for Education "Keeping children safe in education. Statutory guidance for schools and colleges. September 2018. Page 93", the online safety can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes harm.

This e-safety policy should help to ensure safe and appropriate use. One must be aware that different situations happening in the "real world" also happen in the virtual/ Internet World (bullying, radicalisation, abuse).

## Being exposed to illegal, inappropriate or harmful materials

The school has installed a fire wall filter so that we limit the risk of pupil exposure to illegal, inappropriate or harmful materials while they are working on the school's ICT system. Though the school has this, we cannot solely rely on this. Safeguarding children and young people in both the real and virtual world

is everyone's responsibility. E-safety is a child safety issue and it should be an extension of general safeguarding. The pupils are from the beginning taught simple rules for digital communication and how to behave and act responsibly on the Internet and Social Medias.

They will be made aware of dangers that may occur and that they might meet. Also how to act if they experience being bullied, threatened or are being exposed to other negative actions. The teachers will monitor the pupils use of computers throughout the lessons.

Referring to the school's policy of code of conduct; all digital devices (i-Pad, digital watches etc. that may connect with others) should be left at home. The students are not allowed to bring their own devices. This is to make sure that school has control over the use of Internet. Mobile phones must not be in use during school time unless with permission.

## What is the difference between unacceptable and illegal use of the internet?[1]

Illegal usage includes:

- Making, producing or distributing indecent images of children.
- Grooming.
- Making, producing or distributing adult material that breaches the Obscene Publications Act in the UK.
- Accessing, downloading or forwarding criminally racist material.
- Any activity using technology to cause serious harassment, anxiety, alarm or distress which may be contrary to the Harassment or Malicious Communications Acts.

Unacceptable use incudes:

- Making, producing or distributing any materials that are in conflict with the ethos of the school. This will include materials that, while not illegal, contain gratuitous sexual or violent content, incite hatred or which encourage the use of illegal drugs.

## Staff training

Every teacher, employee, parent and pupil at The Norwegian school will know this e-safety policy. It will be reviewed every year at the beginning of the school-year. Parents and pupils will get this as an appendix to the general code of conduct.

## Communications

This table[2] shows how the school currently considers the benefit of using new technologies:

---

[1] http://swgfl.org.uk/FAQs?page=3

[2] Inspired by the Swedish School in London's E-Safety Policy, page 9

| | STAFF AND OTHER ADULTS | | | STUDENTS / PUPILS | | |
|---|---|---|---|---|---|---|
| COMMUNICATION TECHNOLOGIES | Allowed | Allowed if authorised | Not allowed | Allowed | Allowed if authorised | Not allowed |
| Mobile phones may be brought to school | X | | | X | | |
| Digital devices (except mobile phones) that can be used to communicate with others (eg SMARTwatches, i-Pad, PC) | X | | | | | X |
| Use of mobile phones in lessons | | X | | | X | |
| Use of mobile phones in social time | X | | | | | x |
| Taking photos on mobile phones or other camera devices | | x | | | X | |
| Use of hand held devices eg PDAs, PSPs, watches | X | | | | | X |
| Use of personal email addresses in school, or on school network | X | | | | X | |
| Use of school email for personal emails | | x | | | X | |
| Use of chat rooms/ facilities | | X | | | X | |
| Use of instant messaging | X | | | | X | |
| Use of social networking sites | X | | | | X | |
| Use of blogs | X | | | | X | |

## Responding to incidents of misuse

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- radicalisation material
- other criminal conduct, activity or materials

the SWGfL (South West Grid for Learning Trust Ltd.) flow chart (see next page) should be consulted and actions followed in line with the flow chart.

Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the police.

It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If possible, do absolutely nothing to the suspect computer or computers, including turning them on or off.

It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched.

Under no circumstances should the internet safety coordinator, network manager or head teacher attempt to investigate on their own, or bring in an outside "expert" to do so, as this may compromise the evidence if a legal case were to result. In some cases, this may constitute a criminal offence. It is essential that evidence is preserved.

Pupils who have been insulted or affected in any way, should contact their teacher or the school's Designated Safeguarding Lead for further help. They may also call Child Line (0800 1111)or chat/ write e-mail to the Norwegian Kors på Halsen https://www.korspahalsen.no

.

## Consequences

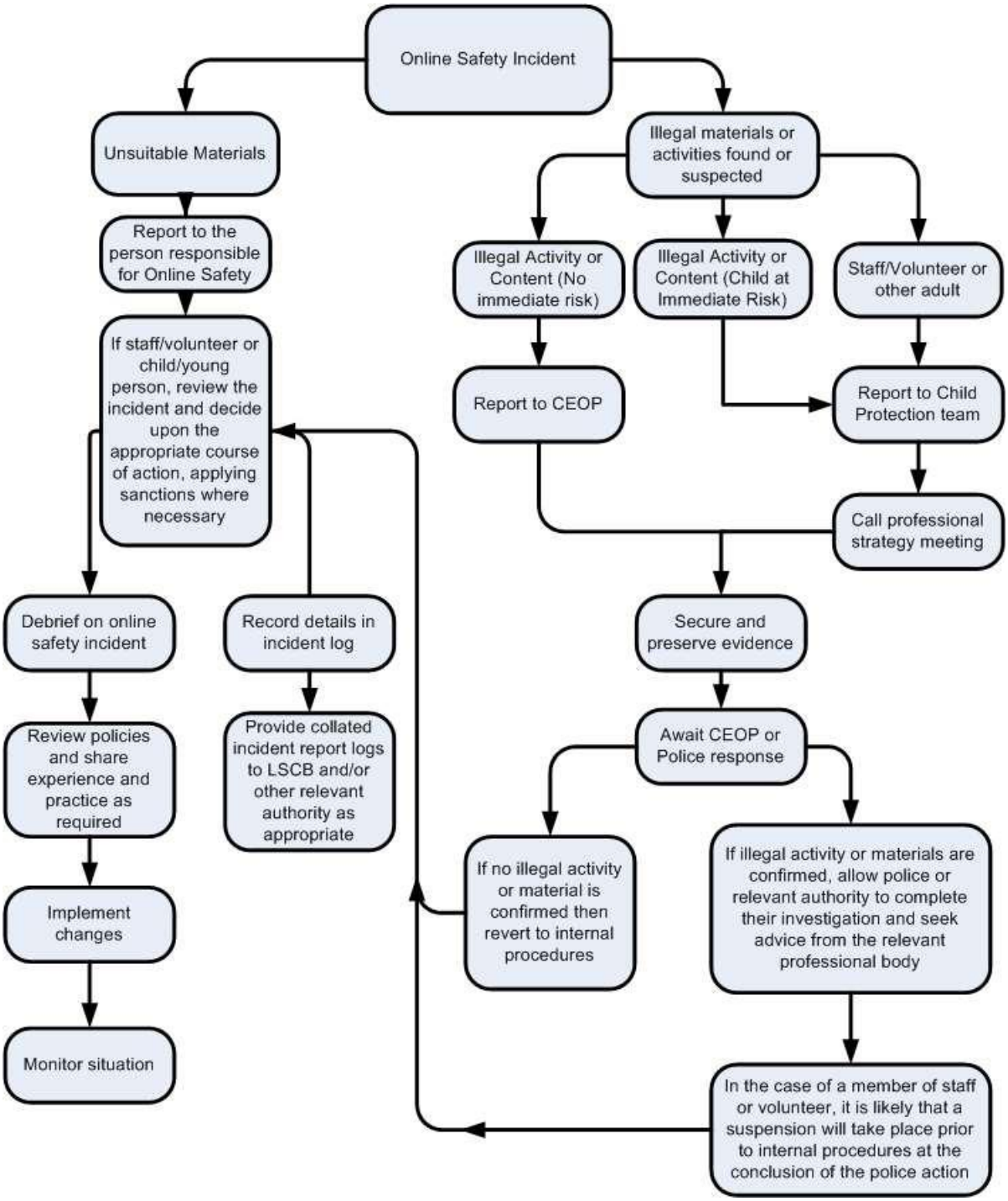
Pupils who uses their mobile phone during school hours (8.45-15.30) without permission:

- First time: The teacher keeps the phone for the rest of the school day.
- Second time: The teacher keeps the phone for the rest of the school day and the pupil must call one of his/ her parents from the office and tell why it has been used.
- Third time: The teacher keeps the phone for the rest of the school day and keeps it until the parents collect it.

Pupils should be aware that any use of the school network may be monitored to ensure appropriate usage. This includes remote scanning of computer monitors, the checking of files and e-mails, and the analysis of internet sites visited. Any attempt to bypass such monitoring is not permitted. The system is monitored by the school's IT-consultant approximately twice a month.

It is important that teachers tell the pupils what the consequences may be if they visit illegal websites, or websites not appropriate for their age. Which consequences the school will effectuate must be agreed with the Head teacher, and parents will be informed. Serious cases will be reported to the police as seen on the flow-chart on next page.

As this policy is an appendix to the school's code of conduct, further consequences is described in the main document.




CEOP= The Child Exploitation and Online Protection Command (Police)
LSCB = Local Safeguarding Children Board (Merton)