E-SAFETY

Review Date: January 2019

Introduction

Our aim through this e-safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike. E-safety is not purely a technological issue. The responsibility for E-safety must not be solely delegated to technical staff, or those with a responsibility for ICT.
We must therefore firmly embed e-safety within all safeguarding policies and practices. The responsibility rest with of all those who work with our pupils whether in a paid or unpaid capacity.

No one policy or technology can create the safe learning and working environment we need. We aim to work towards this by combining the following:

- Policies and Guidance
- Technology Based Solutions
- Education in terms of acceptable use and responsibility

Responsibilities

Headteacher

The Headteacher 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 Network Manager.

The Headteacher and the DDSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).

The Headteacher is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Network Manager.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems

- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students / 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

Network Manager

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority Guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher

- That monitoring software / systems are implemented and updated as agreed in school policies

Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

- The school Acceptable Use Policy (AUP)
- The school Internet Filtering Policy
- The staff Guidance for the Safer Use of the Internet
- The Information Security Guidance

These policies set the boundaries of acceptable use. We need to use these policies however in conjunction with other policies including, but not limited to:

- The Behaviour Policy
- The Anti-Bullying Policy
- The Staff Handbook
- The Staff Code of Conduct
- The Child Protection Policy

Technology

The technologies used to help form a safe environment in which to learn and work include:

- Internet filtering
- Antivirus Software

Education

The education of our pupils is key to them developing an informed confidence and resilience that they need in the digital world. The National Curriculum programme for Computing makes it mandatory for children to be taught how to use ICT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and the professionals who come into contact with children.

Educating our pupils in the practice of acceptable use promotes responsible behaviour and builds resilience. Personal, Social and Health Education (PSHE) lessons also provide an opportunity to explore potential risks, how to minimize these and to consider the impact of our behaviour on others.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, we aim for our pupils to be able to transfer established skills and safe working practices to any new “e-activities” they encounter.

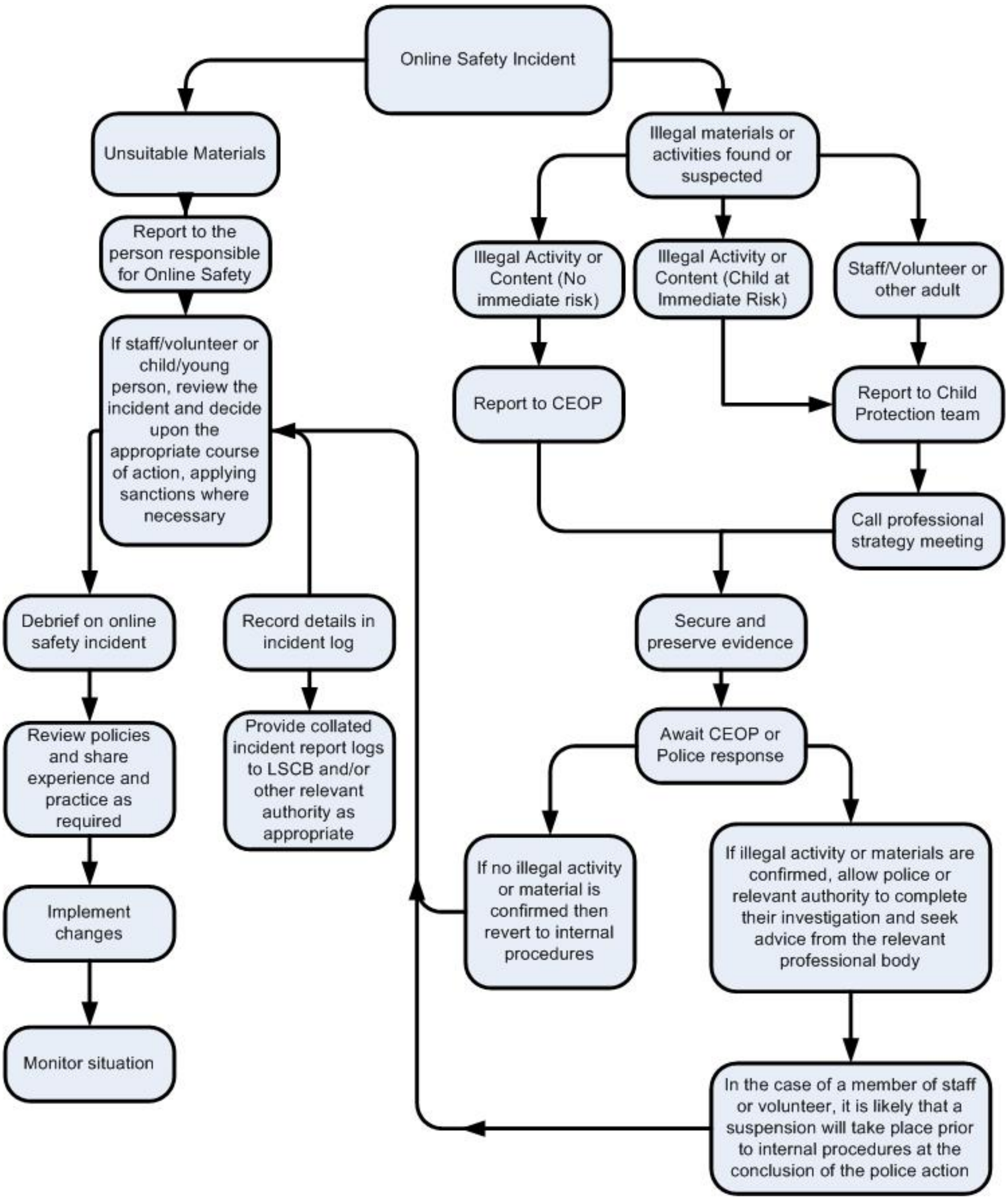
We recognise that it is equally important to ensure that the people who care for our pupils should have the right information to guide and support them whilst empowering them to keep themselves safe.

Monitoring and Self-Review

It is our intention in this time of ever changing technology that we maintain rigorous policies and practices to ensure the e-safety of all our staff and pupils. Our policies will be reviewed on an annual basis and will form part of the induction process for all new members of staff.

Policy written: January 2018
Review Date: January 2019

Responding to incidents of misuse – flow chart


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Littlegreen School
Supporting and developing the whole child

E-SAFETY REPORTING LOG

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		