SOUTH
HUNSLEY

E–Safety Policy

This policy is applicable to: South Hunsley School
Intended audience: Staff, Parents, Students

Important: This document can only be considered valid when viewed on the school website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Simon Windeler, IT Manager
Name of Responsible Committee/Individual:	South Hunsley School and Sixth Form Local Governing Body
Implementation Date:	March 2017
Review Date:	By Spring 2019
Target Audience:	All Staff, Parents, Students

E-Safety Policy

Contents

1. Introduction

Ofsted statements: Online safety is currently covered by the current Ofsted safeguarding guidelines, however: Ofsted have defined e-safety thus (in their previous 'Inspecting e-safety in schools' briefings):

- 'In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.'

E-safety will be inspected in relation to the following areas:

- "The behaviour and safety of pupils at the school.
- The quality of leadership in, and management of, the school"

Ofsted have identified three areas of e-safety risk in relation to pupils:

- "Being exposed to illegal, inappropriate or harmful material.
- Being subjected to harmful online interaction with other users.
- Personal online behaviour that increases the likelihood of, or causes, harm."

An outstanding school will demonstrate that:

- "All groups of pupils feel safe at school and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to e-safety."

2. Aims

This policy aims to set out the school's position in how it will strive to provide an e-safe environment for all of the school community whilst using ICT within the school, and how it will also strive to ensure that its members also use ICT in a safe and responsible manner whilst outside of the school grounds.

This policy will detail the individual responsibilities of each of the key people in the school who have a role to play in fulfilling this policy and its related procedures.
This policy applies to all staff, students, governors and parents of the school community. It should be read in conjunction with the supporting policies and related information that is detailed below.

South Hunsley School believes that ICT can and should be used to enrich the education of all students. ICT also provides the staff of the school with a great many tools to help them play their part in providing the students of the school their education. Whilst the school sees the benefits of using this technology, it is also aware of the potential risks that the internet, ICT and related technology can pose. The school believe that e-Safety is the responsibility of the whole school community, and that all members of that community have their own part to play in ensuring that everyone can gain from the benefits that the internet and ICT afford to teaching and learning, whilst remaining safe.

Social Networking is becoming increasingly popular tool within our environment to support learning and encourage creative use of the internet, and to publish and share content. These technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged.
Although we encourage staff to use social networking to promote learning within school, we also expect staff to maintain a professional level of conduct in their user of these types of technologies.

3. Content

Risks of ICT Use and the Internet

The school has identified the following risks that ICT and the internet can pose to its community: [1]

- Obsessive use of the internet and ICT

[1] This list is by no means exhaustive, but means to highlight some of the main areas of risk that the school has identified.

- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger or sexual abuse
- Being subjected to harmful online interaction with other users.
- Inappropriate or illegal behaviour by school staff

Creating a Safe ICT Learning Environment
The school believes that the best way to provide a safe ICT learning environment is a triple-fold matter:

1. Create an infrastructure of whole school awareness, designated responsibilities, policies and procedures. This can be achieved by:
    - Raising awareness of the risks of technology that is both emerging and already embedded in the school community.
    - Ensuring that the e-Safety policy and education programme adapts to meet these new and emerging technologies and is reviewed as incidents occur.
    - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to e-Safety.
    - Ensuring that the school's policies and procedures are effective and kept up to date, and also make clear to all members of the school community what is acceptable when using ICT and the internet.
    - Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
    - Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
    - Explaining how accessing and / or sharing other people’s personal information or photographs might be inappropriate or illegal.
    - Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
    - Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
2. Make use of effective technological tools to ensure the safe use of the internet and school ICT systems. These include:
    - Firewall protection to the school's network.
    - Virus protection of all relevant IT equipment connected to the school's network.
    - Filtering, logging and content control of the school's internet connection.
    - Monitoring systems.
3. Develop an internet safety education programme for the whole school. This will consist of:
    - An on-going education programme for the students at the school, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the school.
    - Continued Professional Development of all staff to ensure that they are equipped to support the students at the school, and are also fully aware of their responsibilities in using ICT, both in and out of the school.
    - An on-going education programme for parents, carers and the wider community so that they have

the knowledge and tools available to support the actions of the school in these matters.

Executive Principals Responsibilities

1. To take ultimate responsibility for e-safety whilst delegating the day-to-day responsibility to the E-Safety Coordinator (ESC).
2. To ensure that the ESC and the members of the e-safety teams are given enough time, support and authority to carry out their remit.
3. To ensure that the governing body is kept informed of the issues and policies.
4. To ensure that the appropriate funding is available to support the technological infrastructure and CPD training for the e-safety programme.

Governing Body's Responsibilities

1. To ensure the designated Safeguarding Governor considers e-safety as a part of the regular review of child protection and safeguarding.
2. To support the Executive Principal and ESC to ensure that the correct policies and procedures are in place, and also that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of e-safety to parents.

E-Safety Coordinator's Responsibilities

1. To form an E-Safety Management Group to deal with sensitive issues arising from E-Safety in the school.
2. To develop and review the appropriate e-safety policies and procedures.
3. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
4. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of e-safety inside and outside of the school environment.
5. To work with the appropriate members of staff to develop an e-safety education programme for the students.
6. To work with the appropriate members of staff to develop a parental awareness programme for e-safety at home.
7. To maintain a log of all e-safety incidents that occur in the school.
8. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.
9. To meet with the Child Protection Officer regularly to discuss e-safety and progress.
10. To liaise with any outside agencies as appropriate.
11. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Child Protection Officer's Responsibilities

1. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to young people.
2. To act as a key member of the school's E-Safety Management Group and liaise with the ESC on specific incidents of misuse.
3. Take a proactive role in the e-safety education of the school's students.
4. Develop systems and procedures for supporting and referring students identified as victims or

perpetrators of e-safety incidents.

5. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Network Manager Responsibilities

1. To perform regular audits and checks of the school's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the ESC, Head of School and Police if necessary.
2. Review the technological systems upon any discovery or breach of the acceptable use policy, to ensure that the same breach does not happen again.
3. Liaise with the pastoral team if any breach can be traced back to an individual student.
4. Liaise with the ESC and Executive Principal if any breach can be traced back to an individual member of staff.
5. Provide the technological infrastructure to support the e-safety policies and procedures.
6. Reporting any network breaches of the school's Acceptable Use Policy or e-safety Policy to the ESC.
7. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Subject Leaders Responsibilities

1. To work with the ESC to develop an area / departmental policy to ensure that e-safety is embedded in their areas teaching practice.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Heads of House Responsibilities

1. To act as a key member, and first point of contact for the school's e-safety team.
2. To support the ESC in the development and maintenance of appropriate policies and procedures relating to student welfare.
3. To develop and maintain their own knowledge of internet safety issues.
4. To ensure that any incidents of ICT misuse are dealt with through the correct channels, in line with the ICT and e-Safety policies.
5. To ensure that any students who experience problems when using the internet are appropriately supported, working with the ESC and CPO as required.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Special Educational Needs Coordinator Responsibilities

1. To develop and maintain a knowledge of e-safety issues, with particular regard as to how they may affect children and young people.
2. To develop and maintain additional policies and e-safety materials in conjunction with the ESC, tailored to meet the needs of SEN students.
3. To liaise with parents and carers of SEN students to raise awareness of the school's e-safety position and how the parents can support the school's position.
4. To maintain an appropriate level of professional conduct in their own internet use, both within and

outside the school.

Classroom Teachers, Teaching Assistants, LRC Staff and Cover Supervisors' Responsibilities

1. To develop and maintain a knowledge of e-safety issues, with particular regard to how they might affect children and young people.
2. To implement school and departmental e-safety policies through effective classroom practice.
3. To ensure any incidents of ICT misuse are reported through the correct channels.
4. To ensure that the necessary support is provided to students who experience problems when using the internet, and that issues are correctly reported to the ESC and the Student Support Services team.
5. To plan classroom use of ICT facilities so that e-safety is not compromised.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Student Responsibilities

1. To uphold all school e-safety and ICT policies.
2. To report any misuse of ICT within the school to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they or another student experience problems online.
4. To communicate with their parents or carers about e-safety issues and to uphold any rules regarding e-safety that may exist in the home.

Parents' and Carers' Responsibilities

1. To help and support the school in promoting e-safety
2. To discuss e-safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns they may have about their children's use of the internet and technology with the school.

4. Supporting Policies and Related Information

South Hunsley School and Sixth Form College/Education Alliance supporting policies:

- ICT AUP
- Child Protection Policy
- Expectations and Code of Conduct for Staff
- Prevent Policy

5. Procedure for Policy Implementation

The procedural documents for this policy are attached as an appendix.

- Appendix 1 – Procedure for Implementation
- Appendix 2 – e-Safety Incident Reporting Flowchart

e-Safety Policy Appendix 1 - Procedure for Implementation

The school, through the e-Safety Coordinator, will ensure that all staff are aware of the policies and procedures being implemented to meet the e-Safety remit. There will be information available to all staff about the technologies that are already in use at the school as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback into the school's e-Safety discussions, be given clear guidance to what the procedures are and know who they should speak to regarding any issues.

In the first instance, all staff will receive a basic introduction into the e-Safety programme at the school, and be directed towards the resources that have been made available.

An area of the Virtual Learning Environment contains relevant resources and links to information regarding the safe use of new technologies within a school environment. This area also contains documentation of all people’s roles with regards to e-Safety in the school and a clear flowchart of the correct procedures to follow.

The ESC will work with the HR Team and Training Managers to ensure that the school's induction and CPD programmes include adequate provision for the delivery of e-Safety training.

E-Safety will form a part of the Child Protection Induction for new staff starters and direct them towards the existing policies, procedures, resources and course of action.

The additional resources available to CEOP trained staff will be highlighted, and staff will be informed that they are available, but that training is required to use these resources.

Students

The students at the school will be made aware that there is a whole school approach to e-Safety and their roles and responsibilities within this e-Safe environment will be made clear to them. Student members will be invited to participate in the future planning and discussions regarding e-Safety and their opinions will be regularly gauged as to the effectiveness of the provision.

Through individual House assemblies, students will be made aware of policies and methods of enforcing these policies.

The Year 12 students will be made aware of the school's position to e-Safety in their LRC induction programme. A follow assembly will be held for all Year 13 students to make them aware and refresh their memories.

Parents and Carers

The parents and carers of the school will be made aware of policies and procedures and how they can help in ensuring that South Hunsley is an e-Safe school. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

An area on the School's Virtual Learning Environment contains useful links and information for parents and carers regarding e-safety. This area will also contain links to the school's e-Safety policy, the ICT AUP and the Child Protection Policy.

Parental workshops will be delivered to give parents the opportunity to understand e-safety topics and new risks children are opposed to.

Firewall

The school has a perimeter firewall, which is supplied by Smoothwall. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analysed for security audits.

The responsibility lies with the Network Manager and IT Manager for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked.

Anti-Virus Protection

The school has purchased an Enterprise License for Microsoft’s Endpoint Protection. This anti-virus software is installed on all Microsoft Windows based servers and computers on the school network. The VLE web server has ClamAV installed and all uploaded files are scanned for viruses before being accepted onto the servers.

It is the responsibility of the Network Manager to ensure that all necessary computers on the school network are running current anti-virus software and that regular scans are performed. If a virus out-break happens, the Network Manager must notify the IT Manager and the Executive Principal and as soon as possible isolate the infection.

Any devices being brought into to school and connected to the school's ICT network must be proven to have up-to-date Anti-Virus protection and be cleared by the Network Manager or IT Manager before being connected.

Filtering and Logging of Internet Access

The school has a web caching and proxy server that contains accredited filter lists. This enables the school to log all Internet traffic in the school and allow different sites to different groups of users. This server ensures that all internet use on the school's network is logged to an individual user of the network. If the device being used to access the Internet is not a school owned device, the user will have to present valid school network credentials before they can gain any access to the school's Internet connection. If an e-safety incident requires it, all Internet access logs of any student or staff member can be retrieved to support any required processes.

It is the responsibility of the Network Manager to ensure that all computers connected to the school's network only receive an Internet connection by going through the proxy server. The Network Manager, on request of the ESC, will add any sites that have been discovered through e-safety incidents to the block lists of the filtering server. The network manager will perform regular reports from the logs of the web proxy server to present at the e-safety management group, with regards to the most accessed sites and most active Internet users in the school.

Monitoring Systems

The school has many different monitoring system at its disposal;

- All files stored on the school's servers can be searched and checked
- Teachers can monitor the students use of computers within the IT labs they are in
- Every single action performed on the VLE is logged against the user that performed the action. These logs can be accessed to provide evidence for an e-safety incident
- All computer use is monitored centrally against a set of predefined word lists and use or viewing of inappropriate text is logged with a screen grab and the details of the offence, user and time it occurred
- Any incident that has a sanction attached to it is entered into the school's MIS system

The Network Manager will perform a scan of all staff and student home drives for all images and identify any inappropriate images saved. This will be performed once every term and any inappropriate images found, the Network Manager will notify the ESC providing the user name involved, full name of the user, date and time discovered, details of the incident or violation.

The Network Manager will review all users profile pictures and blog entries on the VLE. This will be performed once every term and any inappropriate images found, the Network Manager will notify the ESC providing the user name involved, full name of the user, date and time discovered, details of the incident or violation.

Training in the use of the IT monitoring software will be offered to all staff. The procedure for reporting e-Safety incidents will detail the information needed from staff when reporting an incident recorded by this software.

The monitoring system will monitor all users, staff and students, the same and the client will be installed on all school owned computers. The difference between staff and students, with regards to this monitoring system, will be the method in which those logs are reviewed.

The Network Manager and ESC will access and review the logs of the silent monitoring system for the staff and respond accordingly to any breaches of the AUP or other e-Safety incidents recorded.

Any incident that has a sanction attached will be entered into the SIMS system using a new behaviour type of "e-Safety". These incidents can then be reported upon by the Student Support Services Team and shared with relevant Head of Years and Subject Leaders as required. All e-Safety incidents, regardless of sanction will be recorded by the ESC in the e-Safety incident database in a restricted area of the VLE.

E-Safety Education

Students

All students at the school will receive an on-going e-Safety education programme.

This programme will inform the students of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

The ICT department run a distinct e-Safety unit with every Year 7 student through their ICT lessons. The content of this lesson will be regularly reviewed to ensure that it is in-line with the school's policy and that it contains information about the current and emerging technologies that need to be raised.

The school will follow the Safer Internet Day programme and deliver those resources through year group assemblies. The year group tutors will be informed about the content being delivered, and asked to discuss the content after the assembly is given so that students have an opportunity to raise any concerns or issues from this information.

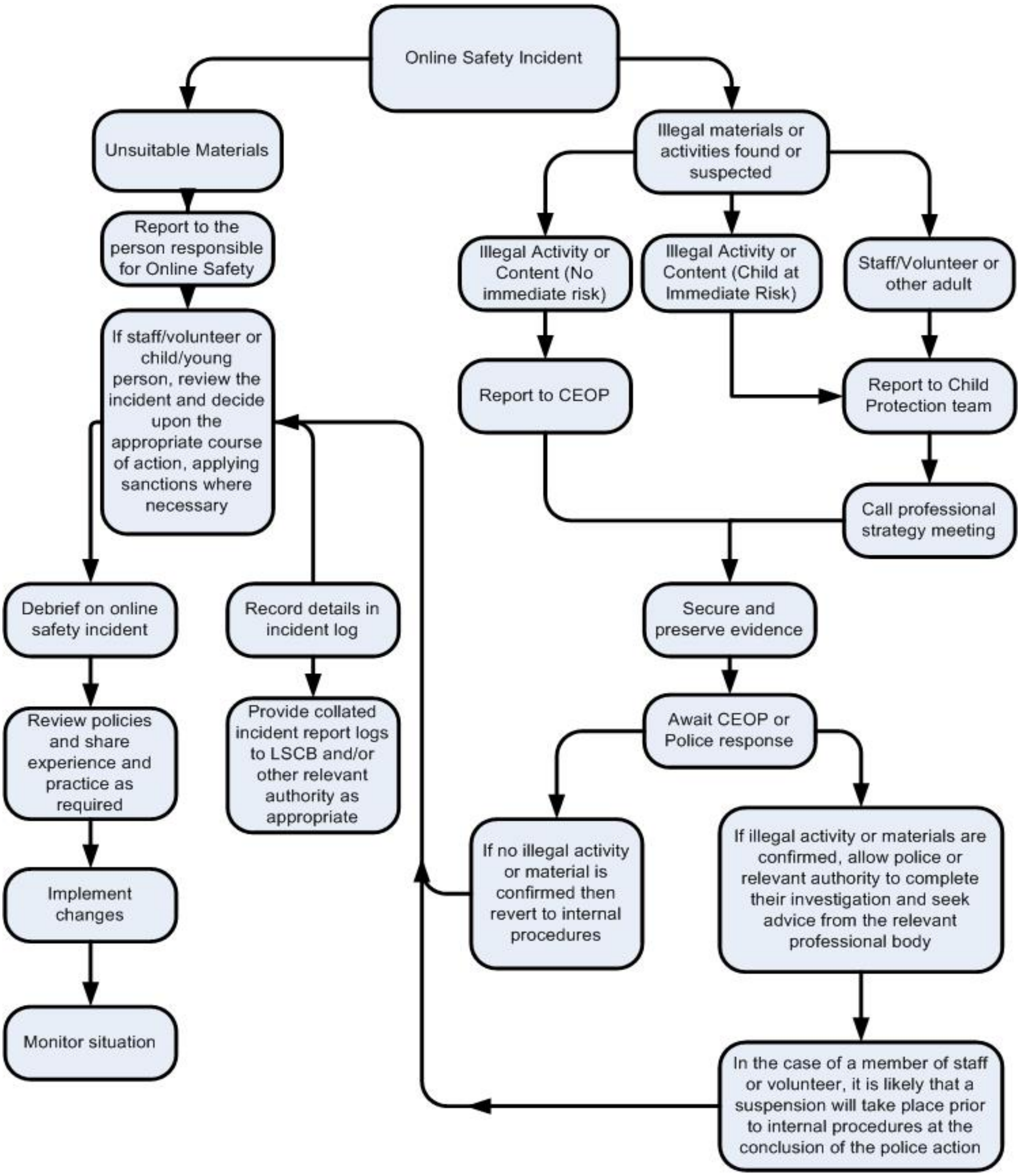
The Post 16 team will work with the ESC to ensure that there is an adequate e-Safety education programme within the Post 16 Curriculum, and that the pastoral support team are up to date with the issues within their area. The e-Safety education programme will be delivered through the Post 16 PSE programme.

The PSE and Personal Development Week curriculum will be regularly reviewed to ensure that it has e-Safety incorporated into its programme.

The SENCO will work with the ESC to ensure that there are accessible and adequate resources available for the SEN students of the school to receive the same e-Safety education as the rest of the school.

The ESC will work with the Pastoral team to ensure there is a commonality of approach in responding to e-Safety incidents and that the correct reaction and procedure is followed by all staff when dealing with an e-Safety issue.

Responding to incidents of misuse – flow chart Appendix 2


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