LEWES NEW SCHOOL

ONLINE SAFETY & ACCEPTABLE USE OF ICT POLICY

POLICY REVIEW INFORMATION:

Policy Reviewed:	**March 2017**
Reviewed by:	Sarah Thomas (Development Manager)
Changes made:	Revised sections relating to Acceptable Use Agreements and use of personal devices to take photos
Policy Reviewed:	**May 2016**
Reviewed by:	Linda Morris (Head Teacher) & Sarah Thomas (Development Manager)
Changes made:	Complete redraft

1. STATEMENT OF INTENT

Lewes New School is an independent primary school and nursery which accepts children from 3-11 years.

The school plays a significant part in the prevention of harm to our students through its **human-centred approach.** The emotional wellbeing of our students is central to this approach. Children can feel safe and be themselves, and relationships are valued and nurtured in a culture of mutual respect.

The school believes it is the responsibility of all members of the school community, including children, staff and parents, to uphold this culture and to work towards ensuring that we can all learn together in a safe environment free from fear.
We recognise that this ethos of care is as relevant to online experiences as it is in other aspects of our lives.

This policy should be read in conjunction with our *Safeguarding Policy*, *Staff Code of Practice*, *Behaviour and Anti-Bullying Policy* and *the Acceptable Use of ICT Agreements.*

2. AIMS & DEFINITIONS

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online-bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

2.1 Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, contractors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of online-bullying, or other online-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will respond to incidents of inappropriate online-safety behaviour that take place out of school in line with its *Behaviour and Anti-bullying Policies.*

2.2 Online-safety Group

The Online-safety Group provides a consultative group that meets to monitor and review the Online-safety Policy and in response to need.

Members of the Online-safety Group include the Headteacher (also E Safety Co-ordinator and Designated Safeguarding Lead), Network Manager, Safeguarding Governor and Student Welfare and E Safety Governor. Other staff and/ or community members are invited to join this group as required.

3. ROLES AND RESPONSIBILITIES

The following section outlines the online-safety roles and responsibilities of individuals and groups within the school.

3.1 Governors

Governors are responsible for ensuring the school has policies and practices in place to keep children and staff safe online.

The role of the Governing Body is to:

1. Approve the Online Safety Policy and review the effectiveness of the policy through regular monitoring reports.
2. Support the school in encouraging parents and the wider community to become engaged in online-safety activities
3. Appoint an Online-Safety Governor to attend online safety review meetings with the Headteacher and class teachers annually or as required

3.2 Headteacher

The Headteacher has a duty of care for ensuring the safety (including online-safety) of members of the school community and has a leading role in establishing and reviewing the school online-safety policies.

The School's Headteacher is also the **Designated Safeguarding Lead (DSL),** and as such is aware that safeguarding action may be needed to protect students from harm.

The role of the Headteacher is to:

1. Lead a ‘safeguarding culture’, ensuring that online safety is fully integrated with whole school safeguarding and promoting an awareness and commitment to online safety throughout the school community.
2. Attend regular training in off-line and online safeguarding, in accordance with statutory guidance Local Safeguarding Children Board (LSCB) guidance.
3. Take overall responsibility for online safety provision, delegating day-to-day responsibility for online-safety to class teachers.
4. Ensure all staff and volunteers receive suitable training and induction to carry out their safeguarding and online safety roles.
5. Be aware of the procedures to be followed in the event of a serious online-safety incident.
6. Ensure online-safety incidents are logged as safeguarding incidents and reported to Governors on a termly basis.
7. Ensure Governors are regularly updated on the nature and effectiveness of the school’s arrangements for online safety.
8. Take overall responsibility for data management and information security (SIRO) ensuring the school’s provision follows best practice in information handling.
9. Liaise with external agencies as required.
10. Liaise with school technical staff and ensure they are fully aware of school online-safety policy and procedures.
11. Meet with Online-safety Governor to discuss current issues and review incident logs.
12. Oversees any community surveys / student feedback on online-safety issues.

3.3 All Staff and Volunteers

All staff and volunteers act as positive role models to students in their use of IT-based technologies.

Staff and volunteers are required to:

1. Promote an awareness and commitment to online safety throughout the school community.
2. Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities, and implement current policies with regard to these devices.
3. Take professional, reasonable precautions when working with students online (e.g. ensuring students’ access to the internet is supervised and via content-filtered log-ins, previewing websites before use).
4. Report any suspected misuse or problem to the Headteacher.
5. Report unsuitable material found in content-filtered Internet searches to the Network Manager.
6. Ensure all digital communications with students / parents / carers have a high degree of professional integrity.
7. At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This includes leaving PIN numbers, IDs and passwords to allow devices to be reset.

3.4 Technical Staff

The school contracts an independent **Network Manager** and **IT Technician** to oversee IT-based technologies at the school.

All technical staff are required to report online safety related issues that come to their attention to the Headteacher.

The **Network Manager** is responsible for ensuring that:

1. The school's technical infrastructure is secure and not open to misuse or malicious attack.
2. Users may only access the networks and devices through a properly enforced password protection policy.
3. The Internet content filtering system is applied and updated on a regular basis.
4. They keep up to date with online-safety technical information in order to inform and update others as required.
5. Software licence logs are accurate and up to date.
6. Any misuse/attempted misuse is reported to the Headteacher.
7. Appropriate backup procedures and disaster recovery plans are in place
8. Up-to-date documentation of the school's online security and technical procedures are in place.

3.5 Teaching Staff

Day-to-day responsibility for online-safety is delegated to class teachers, who are required to:

1. Take day-to-day responsibility for online safety issues and a role in establishing and reviewing the school's Online-Safety Policy.
2. Embed online safety in the curriculum.
3. Supervise and guide students carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant).
4. Ensure that students develop an awareness of research skills and issues relating to electronic content (e.g. plagiarism and copyright)
5. Ensure students understand their roles and responsibilities within the Online-Safety Policy and know how to report unpleasant Internet content or inappropriate use.

3.6 Students

The school has clearly defined expectations of behaviour outlined in our *Behaviour Policy*, which students are expected to adhere to in their behaviour on- and off-line.

Students are supported to:

1. Understand the importance of reporting abuse, misuse or access to inappropriate materials.
2. Know what action to take if they or someone they know feels worried or vulnerable when using online technology.

3. Understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school.
4. Contribute to any 'pupil voice' interviews and surveys that gather information of their online experiences.

3.7 Parents and Guardians

The school works closely with parents and guardians. We will always contact parents with any concerns and hope that parents will share their concerns with the school.

The school recognises that not all parents feel equipped to protect their child when they use electronic equipment at home. The school arranges regular discussion sessions for parents with an external specialist who can advise about potential hazards of technology and practical steps parents can take.

Parents and carers are encouraged to support the school in promoting good online-safety practice in line with this policy and our Parent Consent Form relating to the use of photographic and video images of children.

4. EDUCATION & TRAINING

We believe that technology has the potential to support and enhance teaching and learning for all age groups at the school.

Technologies also bring challenges and risks (as outlined in Section 2). We believe it is essential to balance the use of technology with other tools and experiences for learning, so we carefully consider the introduction of all new technologies.

All our classrooms are equipped with appropriate resources to meet the needs of each age group, including computers and tablets. In addition, all classes have shared access to projection facilities. The school has a responsibility to provide students with quality Internet access as part of their learning experience.

4.1 Teaching Online-Safety

Students are taught and encouraged to act responsibly and with a high level of personal integrity in all their behaviour both on- and off-line.

Our approach to teaching and learning supports the safe and responsible use of IT-based technologies in the following ways:

1. **Students are actively encouraged to think critically:** They are taught to evaluate the integrity of different sources and to recognise that some websites that appear to be impartial may be sources of propaganda (including e.g. racist, homophobic or extremist views).
2. **Students are actively encouraged to be reflective:** They develop self-awareness, an essential prerequisite for developing protective behaviours.

3. **Students are actively encouraged to develop social intelligence**: They develop empathy and an understanding of the consequences of their actions on those around them.
4. **Students are actively encouraged to make mistakes**: They are able to weigh up risks and consider potential outcomes
5. **Students are actively encouraged to trust that their voice is valued**: They feel safe to share their experiences with their teachers and peers.

4.2 Online-Safety in the Curriculum

The school has a flexible curriculum that provides opportunities for:

- whole school, class-based and small-group learning
- teacher-led activities offering age-appropriate skills-based learning
- student-initiated activities that are engaging and relevant to students interests

Online-safety is addressed and reinforced in the following ways through our curriculum:

1. Annual, or more frequent if required, **whole school Online-Safety sessions** with an external specialist provider.
2. Whole school **assemblies** where our key values of care and respect for self and others are reinforced alongside specific online-safety messages.
3. Daily **Circle Time** in each class where our key values are explored and discussed alongside emerging issues in the class including specific online-safety messages.
4. Timetabled **communication and project lessons** where specific skills relating to IT and online-safety are taught and developed in age-appropriate ways.
5. A series of timetabled **transition sessions** to ensure children leave the school with an up-to-date understanding of the issues facing young people today.
6. **Individual** and **small group sessions** with our SENCo or Learning Mentors to support social and emotional learning generally and specifically relating to online-safety as required.

Our online-safety curriculum is reviewed in response to changing guidance and emerging technologies but staff ensure students develop a clear understanding of:

1. The risks associated with the taking, publication and distribution of images of themselves and others online (e.g. on social networking or gaming sites).
2. The risks associated with publishing personal information (including full name, address or school) with any images of themselves or others.
3. The need to implement and maintain privacy settings to keep personal information secure.
4. What they should do if they are subject to bullying or abuse.

4.3 Assessing the Effectiveness of Online-Safety Teaching & Learning

The effectiveness of online-safety teaching and learning is assessed in accordance with our school's *Assessment Policy.*

4.4 Staff and Volunteer Training

The school ensures all teaching staff receive regular, up-to-date online-safety training in order to carry out their responsibilities as outlines in this policy.

An introduction to safeguarding, online-safety and the acceptable use of ICT is provided as part of the induction programme for all new staff and volunteers.

Governors are invited to take part in online-safety training / awareness sessions, both within school and through external agencies.

4.5 Parents' Awareness and Training

The school provides a rolling programme of online-safety advice sessions annually or in accordance with need.

Our weekly Friday Newsletter provides opportunities to share relevant information and to address and reinforce the school's core values generally and specifically relating to online-safety.

5. RESPONDING TO ONLINE-SAFETY INCIDENTS

The school takes all reasonable steps to ensure online-safety and communicate this policy to staff, students and parents. Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online-safety within the school.

There may be times when infringements of the policy could take place through careless, irresponsible or through deliberate misuse. In this instance the school will:

1. Require that any suspected online risk or infringement is reported to Headteacher that day.
2. Ensure that issues are dealt with quickly, sensitively and in a proportionate manner, through the school's escalation processes: *Safeguarding, Behaviour, Complaints, Discipline* and *Whistleblowing Procedures.*
3. Actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues.
4. Informed parents/ carers of online safety incidents involving young people for whom they are responsible.
5. Contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
6. Immediately refer any suspected illegal material to the appropriate authorities (Police and Internet Watch Foundation).

Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors. Concerns will then be referred to the LADO (Local Authority's Designated Officer).

For further guidance refer to:

Appendix A *Responding to Incidents of Misuse flowchart*
Appendix B *Guidance for Reviewing Internet Sites*

5.1 Unsuitable / inappropriate activities

There are a range of online activities which may be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school expects staff to use their professional integrity and good judgement to determine whether or not certain activities (e.g. online shopping or gaming) are appropriate and have educational merit. If in doubt, staff are expected to consult with the Headteacher.

Staff should not use any digital media in any way that may be considered offensive or in breach of the integrity or ethos of the school, or bring the school into disrepute.

6. MANAGING ICT SYSTEMS & DEVICES

The school is responsible for ensuring that the ICT network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This includes ensuring that school technical systems are managed in ways that meet recommended technical requirements and regular reviews and audits of the safety and security of school technical systems are undertaken.

6.1 The ICT Network

All users have clearly defined access rights to school ICT systems:

- All staff and students in Years 3-6 are provided with a username and secure password. Users are responsible for the security of their username and password and asked to change their password regularly.
- Nursery - Year 2 are provided with class usernames and passwords.
- A “Guest” login is provided for temporary access for e.g. supply teachers and visitors onto the school systems.
- The Network Manager maintains an up to date record of users and their usernames.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager are available to the Headteacher and kept in a secure place.

Procedures are in place to ensure the security of school ICT systems:

- Users are asked to log-out of systems when leaving their computer and there is an automatic lock-out for staff after 10 minutes idle time.
- All servers are password protected and managed by DBS-checked staff.
- Users report any actual or potential incident or security breach to the Headteacher.
- Appropriate security measures are in place to protect school ICT infrastructure (including anti-virus software, firewalls and internet filtering software).

- Personal or sensitive data is only stored on the school's secure network or on password-protected devices. Staff are responsible for ensuring the safe, secure use of removable media (e.g. memory sticks / CDs / DVDs) on school devices.

Any personal use by staff on school devices that may be used out of school should be kept to a minimum and within guidelines set out in the *Staff Code of Practice.*

6.2 Online-Safety and Content Filtering

Appropriate precautions are in place to ensure students are not exposed to inappropriate online material but we acknowledge the need to teach students how and why to behave responsibly in order to protect themselves.

- Internet access for all students is filtered using Web Titan.
- Inappropriate Internet content is blocked for all staff by an enforced Google Safe Search facility.
- Content lists are regularly updated and Internet use may be monitored.

6.3 Data Security

All personal data is recorded, processed, transferred and made available according to the *Data Protection Act 1998* which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school has an appropriate *Data Protection Policy* regarding the storage and retention of personal data.

The school ensures that whenever cloud storage is used for storing data, such storage meets the requirements laid down by the Information Commissioner's Office.

Staff are required to:

- Take reasonable care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using secure password protected devices (e.g. memory sticks) and delete data from that device once the transfer is complete.
- Ensure any portable device used to store personal data (e.g. laptops, tablets and hard drives) are password protected and offer approved virus and malware checking software.

6.4 Personal mobile devices

The school acknowledges that certain risks are inherent with staff, parents and students bringing in their own personal mobile devices that are not subject to school's security measures or Internet content filtering.

All reasonable steps have been taken to ensure that data on the school ICT Network is not accessible on personal mobile devices.

- Mobile devices are not permitted to be used in student toilets or when students are changing.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

Mobile devices are brought into school entirely at the staff member, students, parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

Staff use of personal devices

Taking images: The school provides tablets for use in each classroom for the recording and sharing of images, video and audio. The use of personal mobile devices for this is not permitted.

Contacting parents by phone or text: Staff members are expected to use the school phone to contact parents whenever they are on site and to use the school mobile phone to contact parents when off-site.

Contacting students: Members of staff are not expected to have the need to contact students directly by phone or text. If there is an identified need then the Headteacher must be informed.

Use of phones during lesson time or while on duty: Staff are not permitted to use their phones or other personal mobile devices for any reason whilst children are in their care. In the event of exceptional personal circumstances then the headteacher should be informed.

Students' use of personal devices

While the school recommends that student mobile phones and devices should not be brought into school, we accept that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety or wellbeing. In this event parents are requested to inform the school.

Parents are requested not to contact their child via their mobile phone during the school day, but to contact the school office. If a student needs to contact his or her parents they will be asked to use the school phone.

Personal mobile devices should not normally be used during lessons or on school trips. Students' personal mobile devices that are brought into school should be turned off and stored out of sight at the start of lessons.

The school ensures that students and parents understand that personal devices may be confiscated until the end of the day if the student does not adhere to this policy.

7. DIGITAL COMMUNICATION

Any digital communication (including e.g. email, text and social media) between staff and students or parents/ carers should reflect staff professional integrity and good judgment in line with the *Staff Code of practice.*

Staff members are asked to keep professional and private communication separate.

7.1 Email

The official school email service may be regarded as safe and secure. Users should be aware that email communication may be monitored.

Staff emails

Staff should use only the school email service to communicate with others about school-related business.

Users should immediately report to the Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Student emails

Anonymous, whole class email addresses are provided for educational use within school.

7.2 Social Media

We recognise that the school community enjoys open communication, which includes the sharing of individual and community achievements and celebrations online.

All staff, parents and children are expected to use social media in a manner that is respectful to others at all times.

The school ensures all staff, parents and children understand the need to:

- Ask permission before uploading photographs, videos or any other information about other people.
- Not include students' full name, address or personal information with any photographs or videos posted online.
- Not post anything online which may cause embarrassment or offence.

Staff

Staff are expected to ensure that any personal opinions they share are not attributed to the school, do not compromise the professional role of the staff member or bring the school into disrepute.

In addition, staff are advised:

- Not to be online friends with any student (staff should inform the Headteacher of any exceptions to this).
- Not to engage in online discussion on personal matters relating to members of the school community.

For more information see the ***Use of Social Networking and online Media Agreement.***

8. THE USE OF DIGITAL AND VIDEO IMAGES

Photographs and recordings of school activities and community events are highly valued as a vibrant record of school life and may be used to support and document learning or document and promote the school's approach, e.g. on school noticeboards, publicity materials, the school website and in the press.

However, the school is aware of the risks associated with publishing digital images online.

8.1 Acceptable Use Agreements

Staff and parents sign the school's Acceptable Use Agreement forms, which includes a clause on mobile phones/personal equipment for taking pictures.

Students and staff will ONLY use school equipment to create digital images and videos.

Digital images and videos of students are stored in a central location enabling children who have left the school to be easily removed.

Parents may take photographs or videos at school events but must ensure that if they include children other than their own it is solely for their personal use and will not be published on the internet (including social networking sites).

Acceptable Use Agreements are held in the school office. The Bursar is responsible for ensuring all staff are aware of any child for whom consent is not provided.

Please see the ***Acceptable Use Agreement: Staff, volunteers, governors and trustees*** and ***Acceptable Use Agreement: Parents*** for more information.

8.2 Images and Video for School Publication

The school takes steps to protect the identity of all children of whom images are used in school promotional materials and articles, and will only take and use images that are

appropriate and not considered to be open to misuse.

Written permission via a school Acceptable Use Agreement must be obtained from parents and carers before any photographs or videos used:

- On the school's system
- On the school's website or blog
- In display material in and around the school or off site
- In a school prospectus or other printed promotional material

If specific student photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will check with individual parents that they give permission for this additional use.

Where images are used online or in any published school produced video materials/DVDs students will not be identified by name.

Students' names will not be used when saving images in the file names or in the tags when publishing to the school website.

Images of children will be not be retained or used after a child has left the school without the parents permission.

The school ensures that images taken by journalists and other external agencies are subject to the same consents and protective measures as set out above.

For more information see the ***Use of Digital Images and Video Agreement.***

8.3 The Use of Photography and Recording in the Classroom

Photographs and recordings are useful tools for monitoring children's work and progress, and as such form an essential part of classroom life. Photographic images form a useful part of children's individual Learning Portfolios and provide an opportunity for children to reflect on their own personal growth and development.

The school takes the following steps to ensure the safe and appropriate use photography and digital recording:

- Staff discuss the appropriate use of photography with children and supervise any photography undertaken by children in school or during off-site activities.
- Staff ensure all children and adults present are aware of when they are being photographed or filmed, or when a webcam is in use.
- The use of cameras, camera phones or movie cameras is not permitted in toilets, when children are changing or in other situations with a heightened expectation of privacy.
- If cameras, camera phones or movie cameras are misused, the school will follow its usual behaviour and disciplinary procedures.
- Tablets are provided for use in each classroom for recording images and video. The use of staff personal mobile devices for this is not permitted.

9. POLICY MONITORING & REVIEW

The Governing Body will receive a report on the implementation of this policy on a termly basis.

The effectiveness of this policy will be monitored through annual community surveys, internal assessment procedures, incident logs and records of professional development meetings.

This policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online-safety or incidents that have taken place.

10. PUBLICISING OUR POLICIES & PROCEDURES

Lewes New School makes its policies and procedures available to all parents of children and of prospective children on the school's website and in the school office.

On completion or review, all policies and procedures are communicated to all staff (teaching and support staff) and are linked to the induction of all new staff.

11. FURTHER INFORMATION & RESOURCES

www.thinkuknow.com Information and resources for parents, teachers and young people about staying safe online

https://www.ceop.police.uk For advice, help and to report an incident involving a child's safety online

https://www.iwf.org.uk For reporting criminal online content

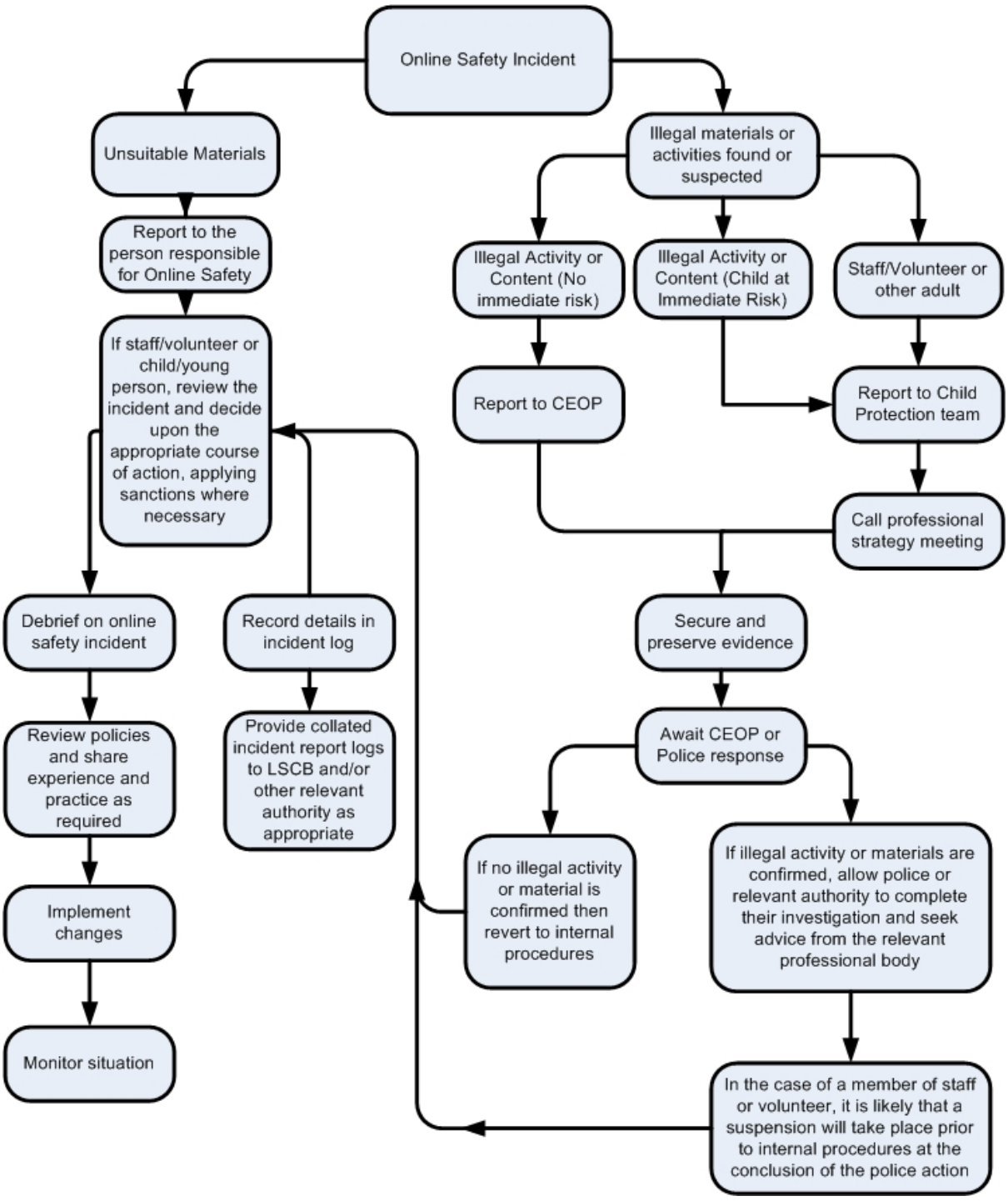
http://www.eastsussexlscb.org.uk ESCC Safeguarding Children Board

11.1 Informing Our Policy

London Grid for Learning Online Safety Policy and guidance

Southwest Grid for Learning E Safety Policy and guidance

Appendix A: Responding to incidents of misuse flowchart



Appendix B: Guidance for Reviewing Internet Sites (for suspected harassment and distress)

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include internet-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police.

Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse3 then the monitoring should be halted and referred to the Police immediately4. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
- **Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix C

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff				Students			
	Allowed	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with Staff permission**	**Not allowed**
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons				X emergency only, agreed by Head in advance				X In line with policy
Use of mobile phones in social time		X out of class, no care of children					X In line with policy	
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices eg tablets, gaming devices		X out of class, no care of children						X Except in exceptional circumstance, under supervision
Use of personal email addresses on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps		X out of class, no care of children						X
Use of social media		X out of class, no care of children						X
Use of blogs		X out of class, no care of children					X	