Staining Road, Staining, Blackpool, FY3 0BW
Tel: (01253) 882983
Email: bursar@staining.lancs.sch.uk
Website: www.staining.lancs.sch.uk

STAINING
CE VC Primary School

STAINING CE VC PRIMARY SCHOOL

Online Safety Policy

Our School Vision:
Learn to Wonder, Grow in Wisdom, Shine Like Stars

At Staining CE Primary School, we have five key values that permeate all aspects of school life. They are:

- Work Hard
- Aim High
- Show Respect
- Be Kind
- Teamwork

Through actively promoting, teaching and prioritising these values across all aspects of school life, and through this policy, we aim to ensure that every member of the school community feels valued and respected, and that each person is treated fairly. We are a caring school. These values are underpinned by our Christian values and it is through the teaching of these that they become meaningful to the pupils.

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, visitors, 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 Head teachers to such extent as is reasonable, to regulate the behaviour of pupils 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 cyber-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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The head teacher has overall responsibility. The Online Safety Officer (Deputy Head) will manage the day-to-day responsibility for Online Safety. It is the role of these staff members to keep abreast of current issues and guidance. The Head teacher ensures that the Senior Leadership Team and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school online safety procedures. All staff should be familiar with the school's policy including:

- Safe use of email

- Safe use of the Internet
- Safe use of the school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs on the school website
- Procedures in the event of misuse of technology by any member of the school community (see appendices)
- Their role in providing online safety education for pupils.

Staff are reminded/updated about online safety regularly and new staff receive information on the school's acceptable use policy as part of their induction.

Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see appendices).

In managing the school online safety messages:

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The online safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- Online safety posters will be prominently displayed.

Governors / Board of Directors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor . The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Online Safety Officer:

The Online Safety Officer:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority / relevant body
- Liaises with school technical staff

- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to the head teacher

Network Manager / Technical staff:

The school has a managed ICT service provider from an outside contractor. It is the school's responsibility to ensure that the managed service provider carries out all the online safety measures. The managed service provider will be made fully aware of the school's online safety policy and procedures. The Network Manager / Co-ordinator for ICT / Computing 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 / other relevant body Online Safety Policy / Guidance that may apply.

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 children with quality Internet access as part of their learning experience. Internet use is a part of the daily life, the curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The school internet access is designed expressly for pupil and staff use and includes 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.

Using the internet

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
- The use of the internet, e-mail, or any other media to access inappropriate materials such as gambling, pornography, racist or any other offensive material is strictly forbidden;
- Personal use of the school internet is only acceptable in non-teaching time, i.e. before or after school and in designated breaks.
- It is the responsibility of the user to ensure that they have logged off sites when they have completed tasks.

The school reserves the right to examine and move files that may be held on its computer systems or to monitor any internet sites visited and other usage of computing resources.

Authorisation of access to the internet

Access to the Internet is under direct adult supervision, with children using filtered search engines. All webpages used for learning will be vetted by the teacher before lessons. During lunchtimes and in Breakfast and After School Club, either in the ICT suite or on IPads, pupils are not permitted to carry out Google searches; but only permitted to use pre-approved apps that are uploaded onto devices.

Using the Internet to Enhance Learning

- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.
- Children are educated in the safe use of the internet at the beginning of each school year and will be given further discrete sessions during the remaining terms as part of the PSHE and Computing curriculum. This is supplemented by online safety reminders whenever computers are used.
- Pupils use a range of internet resources such as Purple Mash, Edshed, Times Tables Rockstars, REN Learning, Studyladder, Lexia, SPAG.com and others. All children have their own access codes as appropriate. Children are aware that they must not share their password or personal information with anyone else.
- Pupils are taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information and to respect copyright when using internet material in their own work.
- Children must not be given unsupervised access to the internet. For the purposes of this policy, 'supervised' means a directed task or access to a specific website.
- The teaching of online safety is included in the school's curriculum. All year groups discuss online safety issues as part of the responsible use of the school's computer systems; information for parents and children can be accessed via our school website. Children are aware of where to seek help and who to report abuse to if necessary.
- All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.

Management of filtering

Broadband connection, filtering and virus protection is provided by BT Lightspeed. Netsweeper runs the filters and Sophos is the anti-virus software. These systems are managed by LancsICT.

- If staff or pupils discover unsuitable sites, the web page will be minimised. When safe to do so, the teacher should then open the page and make a note of the URL (address) and content of the site and report it immediately to the designated administrator. This will then allow access to this site to be blocked in future
- If appropriate, changes to the search filtering rules and website filter can be made. Dates of any changes and reasons for these must be recorded and reviewed regularly
- Staff need to report suspected computer virus infection directly to the Headteacher/ Computing Subject Leader who will report it to the relevant body/ technical support.

Use of school equipment

Equipment such as laptop computers and iPads are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use Policy. The equipment is fully insured from the moment it leaves the school premises. ***Note:*** Our school insurance policy provides cover for equipment taken offsite, provided it is looked after with due care, i.e. not left in view on a car seat, etc. GDPR and data protection issues if a device is taken offsite: refer to policies.

Management of the school website

The administrator password for the school network is available to the head teacher, deputy, Computing lead and the network management. Technicians liaise directly with the Computing Subject Leader and head teacher, who will ensure that technical issues are dealt with quickly and appropriately.

The website domain name is owned and operated by Lancashire. Website hosted on a private UK based at UKFAST Campus, Birley Fields, Manchester, M15 5QJ Manchester and managed by Superchance Ltd. A copy of the I.P address is kept in the school office.

No secure data is used on the website.

The point of contact on the school website will be the school address, school email and telephone number. Staff or pupils` home information will not be published. The website is maintained and updated by the head teacher or delegated staff member but the head teacher has overall responsibility for ensuring the content is appropriate and current. Regular audits of the school website will take place during the year to ensure that documents and links are up to date and in-line with all statutory rules.

- Website photographs that include pupils are selected carefully. Names are not associated with photographs.
- Pupils` full names are not used anywhere on the website.
- Permission from parents/carers for photographs of pupils to be published on the school website, or any other sites for educational purposes, is obtained at the start of each school year. The photograph permission slips are checked before photographs are used in order to ensure that there are not children whose parents who have NOT given permission for their child(ren)'s photographs to be used on the internet in the group.
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.
- Downloadable materials are in PDF format to ensure the content is not manipulated and distributed without the direct consent of the school.

Staff Training

Online safety training is carried out on an annual basis, and more frequently as required. The HT as DSL has attended online safety training and disseminates this information to colleagues as necessary.

Members of staff are made aware of the implications of using social networking sites (including online chat platforms) and do not use these to contact pupils, either past or present or upload any contact that refers directly to the school, pupils or other members of staff. See Staff Social Media Policy.

Mobile devices

The use of mobile devices by pupils in school is not permitted. If they are brought into school, they must be handed into the class teacher until leaving the premises. Staff may bring mobile phones into school, but they are not to be used in the classroom or staff room. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or kept on silent at all times.

If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved in advance by the senior leadership team.

Photographs of children may not be taken on staff phones in order to prevent photographs of children leaving the school premises. School cameras should not be taken off the premises other than for educational trips and, once used, photographs of children should be deleted from the memory. Where teachers use their staff iPad for taking photos of children, they should ensure that the device remains password protected. Personal cameras should not be brought into school or used to photograph children. Photographs and video of pupils and staff are regarded as personal data and written permission is obtained for their use from individuals and parents/ carers before they are published on the website, in brochures, or for display.

Social networking and personal publishing

- Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces e.g. Facebook is inappropriate for pupils aged 12 or under.
- Pupils will be taught lessons specifically dealing with these issues via the Purple Mash platform and school curriculum.

Staff use of Email

The Freedom of Information Act 2000 legislation categorises email with all other forms of written communication, making it a criminal offence to alter, delete or conceal information to prevent disclosure. Staff should therefore only include information in an email that they would send in letter format, and be mindful that any information could enter the public domain at some point.
All users should be aware that email communications may be monitored at any time in accordance with the Acceptable Use Policy.
All users should report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Pupils are taught to use email in accordance with our Online Safety Policy via the Purple Mash platform and are reminded at the beginning of every lesson about online safety issues.

Accounts are deleted for staff who leave the school and this is the responsibility of the Headteacher in conjunction with technical support.

School Website

The school website is used as communication and learning tool. The Head teacher has access to all areas of the school website and may delegate its day-to-day upkeep to members of staff.

Online Communication Tools

Zoom and Class Dojo are used as the school's remote learning platform. Permission must be received prior to using with pupils. Protocols must be followed in line with school's Zoom risk assessment which can be found on the school's website. Zoom is also used as a remote staff meeting tool and training is given to all staff prior to its use.

Remote Learning

In response to the COVID-19 pandemic, the school is likely to establish a platform for providing some face-to-face contact between children and teachers. This will be done in consultation with the LEA and the DfE, as well as parents. All interaction will take place on Zoom. Parents will be made aware of planned meetings in advance, and where possible, school will establish a regular timetable to help support consistent routines at home. Please see Zoom Risk Assessment.

Teachers will commit to the following when contacting children:

- Only use Class Dojo accounts
- Contact should be arranged in advance and be used to provide educational or pastoral support, only
- All contact will take place during normal school hours
- If sharing any content via 'screen share' ensure all non-essential windows are closed

Children will commit to the following when joining video meetings:

- Only use their Class Dojo account
- Use a device in a neutral part of the house, never bedrooms or bathrooms
- Do not have anything in the background which might give away address or other personal information
- No other children under 16 to be on the camera

Parents will commit to the following when their children attend online meetings:

- To supervise their child's use and conduct during the meeting

Access to unsuitable material - Dealing with incidents

Teaching and Support Staff

All staff will be given the school Online Safety Policy to read and sign and its importance will be explained. Staff should be aware that Internet traffic can be monitored and is not only traceable to the individual user, but also the location. Discretion and professional conduct is essential. All 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 (AUP)
- They report any suspected misuse or problem to the Head teacher or Online Safety Officer for investigation / action / sanction
- 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
- Students / pupils understand and follow the online safety and acceptable use policies
- Students / 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 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

Students / pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (see appendix 2 for Pupil Acceptable Use Agreement)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting 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, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems (see appendices).

Education - pupils

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum. The online safety curriculum will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies / the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. This will also be monitored by the headteacher via weekly internet activity reports.

Education - parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education - The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision (supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be: Please refer to the school's GDPR policy.

- 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 must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data

- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office

Information Commissioner's Office

Staff must ensure that they:

- At all times take 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
- When personal data is stored on a portable computer system, memory stick or any other removable media:
    - the device must be password protected
    - the device must offer approved virus and malware checking software

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk. School staff should ensure that:
    - No reference should be made in social media to students / pupils, parents / carers or school staff
    - They do not engage in online discussion on personal matters relating to members of the school community
    - Personal opinions should not be attributed to the school or local authority
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance with the Social Media and Data Protection Policies

Handling Online Safety Complaints

Complaints of Internet misuse will be dealt with by the Online Safety Officer or Head teacher. Any complaint about staff misuse must be referred to the Online Safety Officer. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Please see Online Safety Report in appendices.

Standards and inspections

In order to ensure that the policy is having the desired effect, incidents will be monitored and reviewed on a termly basis and analysed to establish any recurring patterns. This is carried out by the Computing Subject Leader and the senior management team.

Before new technologies are introduced, a risk assessment takes place and any issues will be added to the policy: members of staff, parents and governors are informed.

Appendix

1. Online Safety Incident Report
2. Responding to incidents of misuse

APPENDIX 1

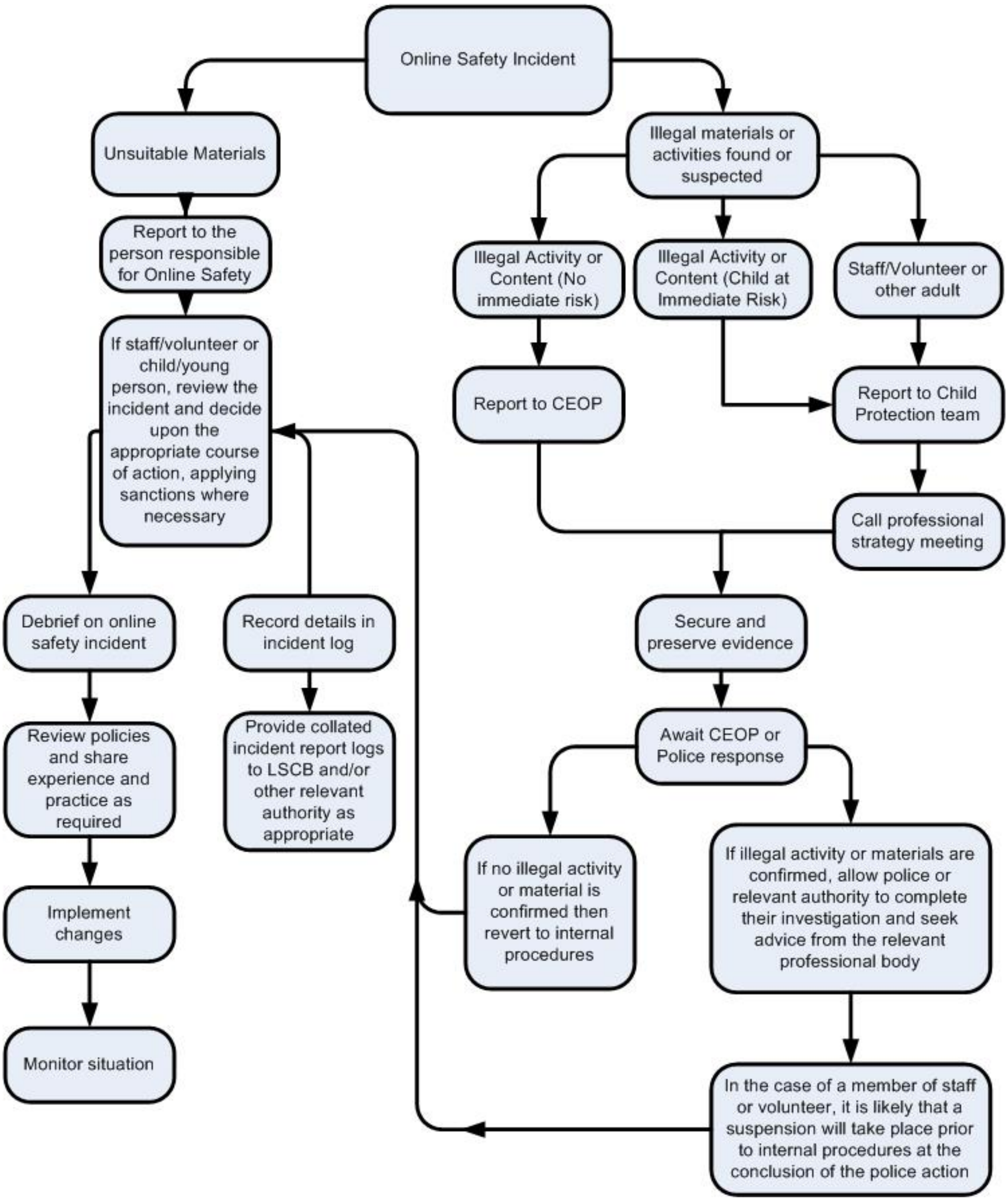
Staining Primary School Online Safety Incident Log

Details of ALL online safety incidents to be recorded in the Incident Log by the Online Safety Officer. This incident log will be monitored termly by the Online Safety Officer and Head teacher.

Date & Time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of Incident (including evidence)	Actions and Reasons

APPENDIX 2

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