E Safety Policy

Development / Monitoring / Review of this Policy

This policy has been developed with 2016 statutory requirements which requires the Board of Governors and Principals to consult with all key stakeholders (pupils, parents and staff) regarding safety issues.

Consultation with the whole school community has taken place through a range of formal and informal meetings and questionnaires.

This Online Safety Policy will be approved by the Board of Governors. It will be monitored at regular intervals, it will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats online safety or incidents that have taken place.

Should serious online safety incidents take place, the following external persons / agencies should be informed:

- Child exploitation and online protection, PSNI, CCMS, Education Authority and Department of Education Northern Ireland, (safeguarding in the board)

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of pupils / parents / staff

  This policy applies to all members of the Our Lady of Lourdes Primary School, pupils, volunteers, parents / carers; visitors who have access to and are users of our school ICT systems, both in and out of the school.

  The school will deal with such incidents within this policy and associated behaviour and anti-bullying discipline policies, C2k agreements, Acceptable Use Policy and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place in our school.

- Acceptable use Policy will be in place for school community.

Roles and Responsibilities

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

Governors

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 (a subcommittee) receiving regular information about online safety incidents and monitoring reports. The role of the Online Safety Governor will include:

- Organise and attend regular meetings with the Online Safety Co-ordinator / Officer
- Attendance at Online Safety Group meetings
- Safeguarding subcommittee
- Regular monitoring of Online Safety incident logs
- Reporting to relevant Governors
- Principal has a duty of care for ensuring the safety (including online safety of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator / ICT co-ordinator.
- The Principal / Senior Management Team are responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive relevant training to enable them to carry out their online safety roles and train their colleagues, as relevant.

Online Safety Co-ordinator Mr McQuaid / Mrs Gribbin

- 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 procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with 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.
- Attends relevant meetings.
- Reports twice per year or as needs arise from specific incidents to Senior Management Team.
- Be aware of personal devices (staff) accessing internet.
- Children should never access unsupervised.

Our school has opted into ‘Securus’ which monitors the screen display and keystrokes of students on C2K managed machines. It triggers a capture if the content is listed in the database of inappropriate words and phrases.

ICT Co-ordinator

As the school has a managed ICT service provided by an outside contractor (C2K) it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the school Online Safety Policy and procedures.

The Co-ordinator for ICT is responsible for ensuring:

- That the school's technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets the required online safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Online Safety Co-ordinator.
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement.
- Understand use / mis-use of social Media e.g. Facebook, Snapchat, Twitter
- They report any suspected misuse or problem to the Principal / Online Safety Co-ordinator for investigation.
- 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 Policy and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They monitor the use of digital

technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- In lessons where internet use is pre-planned 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.
- Staff need to be conscious of the internet options on their devices.

ICT Committee / Online Safety Group – IT Panel

The Online Safety Group provides a consultative group that has wide representation from the school community, Years 1 – 7, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Co-ordinator with:

- The production / review / monitoring of the school Online Safety Policy / documents.
- Overseeing the C2K filtering policy.
- Mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network / internet / incident logs.
- Consulting parents / carers and the students / pupils about the online safety provision.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Have 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 how 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.
- 'Guidelines for Pupils' Internet Access'.

Parents / Carers – Annual agreement with school. (Signed annually)

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 / carers understand these issues through parents' evenings, newsletters, letters, website / Learning Platform 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 follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website / Learning Platform.

Policy Statements

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore 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 should focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for 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 and 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg. Racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Technical Staff (ICT co-ordinator) can temporarily remove these sites from the filtered list for the period of study. Any request to do so, should be auditable,

with clear reasons for the need. Request should be communicated to IT co-ordinator / Principal.

- Acceptable Use Policy displayed in classes and referred to.

Education – Parents / Carers

Many parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in 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 how to respond.

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

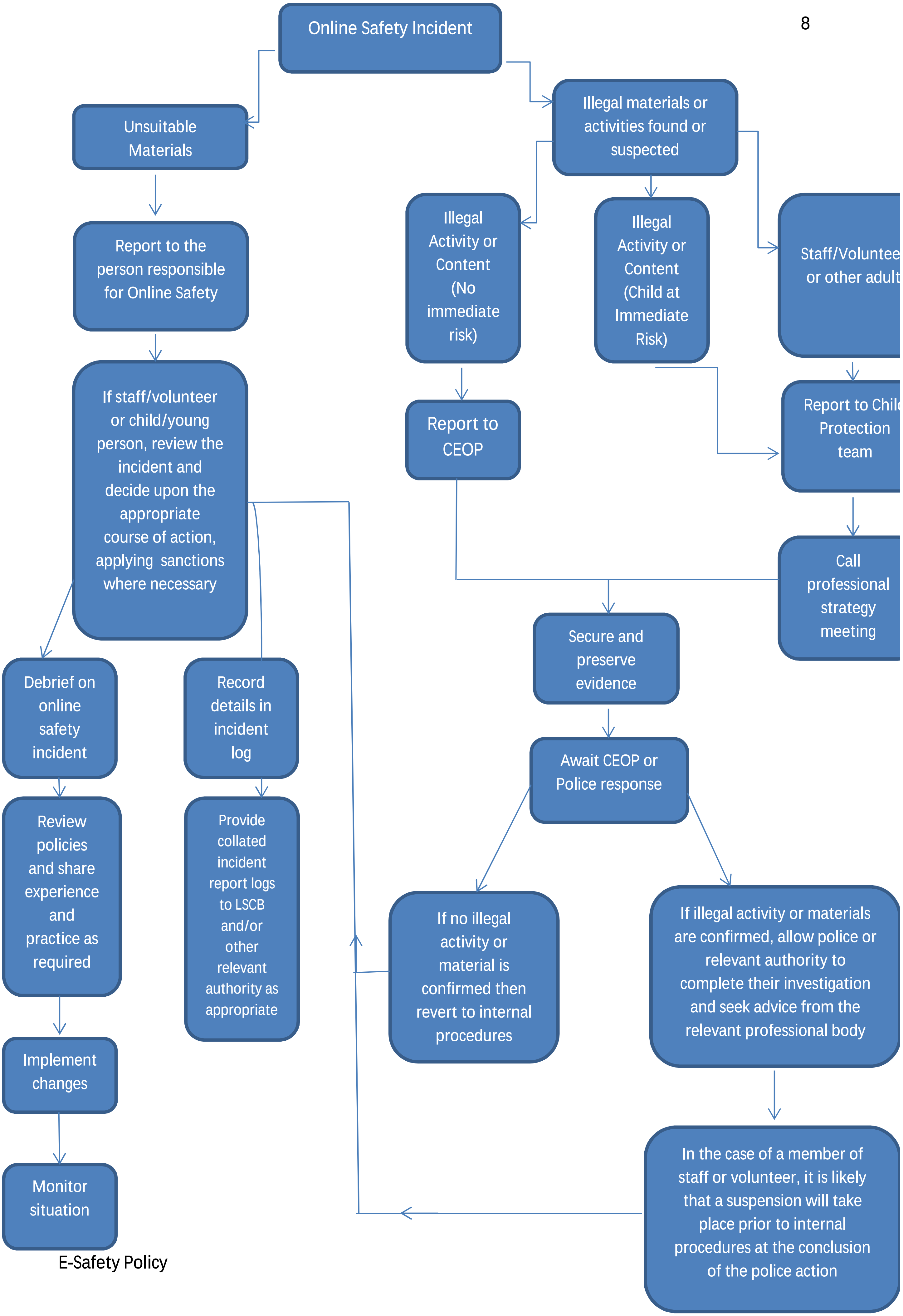
- Curriculum activities.
- Letters, newsletters, web site, Learning Platform.
- Parents / Carers evening / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk / http://childnet.com/parents-and-carers

Technical – infrastructure / equipment, filtering and monitoring

As the school has a managed ICT service provided by an outside contractor, (C2K) it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / Academy Group / other relevant body policies on these technical issues.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by relevant individual who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 3 months.

- The ‘Administrator’ passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Principal.
- School website.
- School website makes use of Twitter which is closely monitored.



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)

Report to CEOP

Illegal Activity or Content (Child at Immediate Risk)

Staff/Voluntee or other adult

Report to Chil 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