The Weston Federation

Weston Infant and Weston Junior Academy

E-Safety Policy

Scope of the Policy
This policy applies to all members of the *academy* community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the *academy*.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the academy. 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 *academy* 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 e-safety behaviour that take place out of school.

What is E-Safety?
E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End E-Safety
E-Safety depends on effective practice at a number of levels:
Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
Safe and secure broadband including the effective management of filtering.

Reviewing the E-Safety policy
The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection (safeguarding). The ICT curriculum coordinator will also act as E-Safety coordinator. The E-Safety Policy and its implementation will be reviewed annually.

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 pupils with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
Internet use will enhance learning.
The school Internet access will be designed expressly for pupil use and will include 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.

Managing Internet Access
Information system security.
School ICT systems capacity and security will be reviewed regularly.
Virus protection will be updated regularly.
Security strategies will be discussed within Saint Bart's Trust.

E-mail
(Currently blocked and only opened if Teacher requests e.g. covering within the curriculum)
Pupils may only use approved e-mail accounts/messaging systems on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school learning platform
The contact details on the Web site must be the school address, e-mail and telephone number.
Staff or pupils' personal information will not be published.

Publishing pupils' images and work
Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. (No children's names to be used).
Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school Web site. This is done on entry to school.
No photographs of Looked after Children should be displayed.

Social networking and personal publishing
The school will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering
The school will work with the LA, Stoke on Trent Safeguarding board and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator. (Sharon Brown/ David Smitten who will directly report to SLT and block accordingly).
The ICT co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions
Authorising Internet access
All staff must read and adhere to the acceptable use policy before using any school ICT resource.
Access to the Internet will be by supervised access to specific, approved on-line materials.
All staff must read and understand the related computing policies (see Related policies).

Assessing risks
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor local authority can accept liability for the material accessed, or any consequences of Internet access. If unsuitable material appears, the E-Safety coordinator & SLT will be informed so that relevant filtering can be completed.
The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints
Complaints of Internet misuse will be dealt with by the class teacher and where necessary a senior member of staff. Teachers to log the incident in their report log and follow the 'responding to incidents of misuse flow chart' (see attached documents).
Any complaint about staff misuse must be referred to the Head teacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet
External organisations using the school's ICT facilities must adhere to the E-Safety policy.
Internet use by staff and children is actively monitored.

Communicating the E-Safety Policy
Introducing the E-Safety policy to pupils

E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and throughout the year as part of computing and PHSE sessions.
Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy
All staff will be given the School E-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support
Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school learning platform.

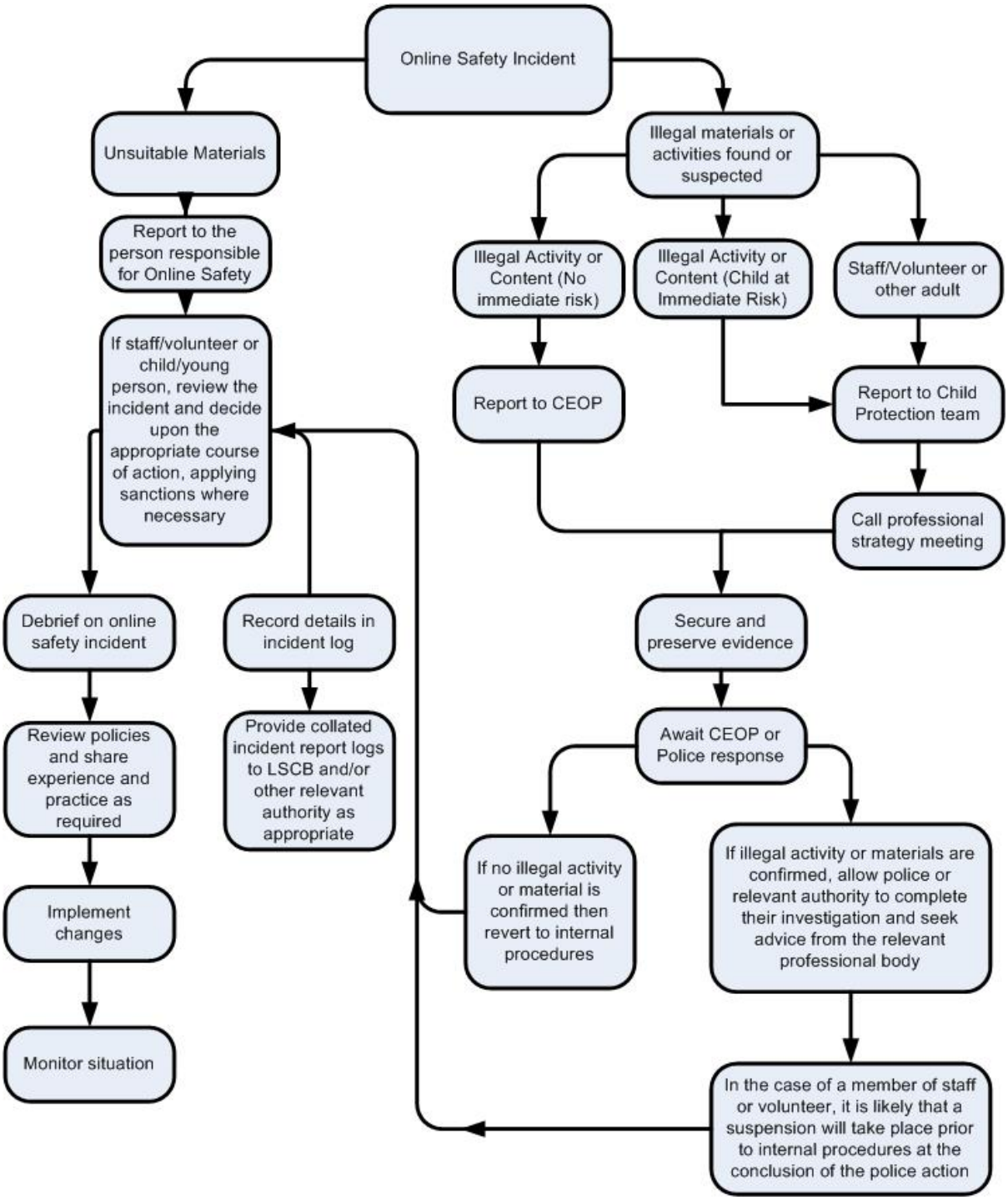
Radicalisation and Extremism
Weston Federation takes an active role in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. In the same way teachers are vigilant about signs of possible physical or emotional abuse, we are vigilant about any signs of radicalisation or extremism in any of our pupils. We follow the same safeguarding procedure to ensure all children in our care are well looked after. For more information on Radicalisation and Extremism please follow the link on our website on the e-safety page.

Related policies
There are a number of other policies at Weston Federation which relate to the topics mentioned above. It is important that you read and fully understand the polices below which can be found on the Weston Federation website. If you have any questions about this policy or any other policies please ask Mrs. Brown or Mr Smitten.

- Staff and volunteer acceptable use policy
- Parents acceptable use policy
- Use of digital and video images
- Pupil acceptable use policy
- Social media policy
- Mobile device policy
- Filtering policy
- Data protection policy

Date of next review September 2021

Responding to incidents of misuse – Flowchart



Weston Federation Reporting Log
Name .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		