Wedmore First School Academy & Nursery

E-Safety Policy

Date: April 2016

Wedmore First School Academy & Nursery

E-Safety Policy

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and acceptable use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individuals' consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inablility to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This e-safety policy has been developed by a working group made up of:

- School E-Safety Co-ordinator
- Headteacher/Leadership & Management Team
- Teachers
- ICT technical staff

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Governors' curriculum committee
- School website/newsletter

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Co-ordinator/Leadership & Management Team/Governors' Curriculum Committee
Monitoring will take place at regular intervals	Annually
The Governing Body/Curriculum Committee will receive a report on the implementation of the e-safety policy at regular intervals	Annually
The e-safety 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 e-safety or incidents that have taken place. The next review date will be:	November 2016

Should serious e-safety incidents take place, the Community Police following external persons/agencies should be informed	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL (South West Grid for Learning) monitoring logs of internet activity (including sites visited)
- Internal monitoring for network activity
- Surveys/questionnaires – pupils/parents/carers/staff

Scope of the Policy

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

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 school 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 out of school, but is linked to membership of the school.

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 e-safety behaviour that take place out of school.

Roles and Responsibilites

The following section outlines the roles and responsibilites for e-safety of individuals and groups within the school:

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

- Regular meetings with the E-Safey Co-ordinator
- Regular monitioring of e-safety incident logs
- Reporting to relevant Governors' committee / meeting

Headteacher and Leadership & Management Team (LMT)

- The Headteacher is responsible for ensuring safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety co-ordinator.
- The Headteacher / LMT are responsible for ensuring that the E-Safety co-ordinator and other relevant staff receive suitable CPD (Continuing Professional Development) to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / LMT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The LMT will receive monitoring reports from the E-Safety Co-ordinator.
- The Headteacher and another member of the LMT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see SWGfL flow chart on dealing with e-safety incidents included in a later section – "Responding to incidents of misuse" and HR / disciplinary procedures).

E-Safety Coordinator: (Jo Bradshaw)

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with e-safety governor to discuss current issues, review incident logs and filtering/change control logs
- Reports regularly to the LMT

ICT Co-ordinator/Technical staff:

The ICT co-ordinator and ICT technician are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage policy
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to filtering applied by the Grid
- That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network/website/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety co-ordinator/Headteacher/Deputy Head/ICT co-ordinator/class teacher for investigation/action/sanction
- 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 e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the e-safety co-ordinator/Headteacher/Deputy Head for investigation/action/sanction
- Digital communications with pupils should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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

Designated person for Child Protection/Child Protection Officer: (Jackie Hipwell)

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement (AUP), which they are taught to understand and respect through e-safety specific lessons as well as regular reminders during other teaching sessions as appropriate.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, the school website and information about national/local e-safety campaigns/literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Home/School Agreement
- Accessing the school website/school records in accordance with the relevant school AUP.

Policy Statements

Education – pupils

Whilst regulation and technical support solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-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 helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/internet (Click Aware) will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential part in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide." (Byron Report)

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

- Newsletters/website
- Parents' evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and AUPs
- The e-safety co-ordinator will receive regular updates through attendance at SWGfL information/training sessions and by reviewing guidance documents released by SWGfL and others.
- This e-safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The e-safety co-ordinator will provide advice/guidance/training as required to individuals as required.

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of the e-safety committee. This is currently the curriculum committee with Steven Willis as e-safety governor. Governor training will be achieved through participation in school training/information sessions for staff/parents.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and AUP and any relevant local authority e-safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password
- The ‘administrator’ passwords for the school ICT system, used by the Network Manager (or other person) must also be supplied to the Business Manager or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the e-safety co-ordinator and SLT. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the e-safety committee.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the AUP.
- An appropriate system is in place for users to report any actual/potential e-safety incidents to the e-safety co-ordinator or SLT.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place regarding the extent of personal use that users (staff) and their family members are allowed on laptops and other portable devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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, eg using search engines, 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) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT co-ordinator can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be recorded in the filter log, with clear reasons for the need.
- 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.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles

- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students / Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any loss, theft, change of ownership of the device will be reported to school.

Use of digital and video images – photographic,video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 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.
- Staff 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.
- Pupils and parents who take photographs, for example on a school trip or a community event must not 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, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

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:

- 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' (See appendix 1 of Data Protection Policy).
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- 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 procedure 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

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.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected
    - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice;

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and politely and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and academies have a duty of care to provide a safe learning environment for pupils and staff. Schools and academies 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 / academy 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 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

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 academy
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

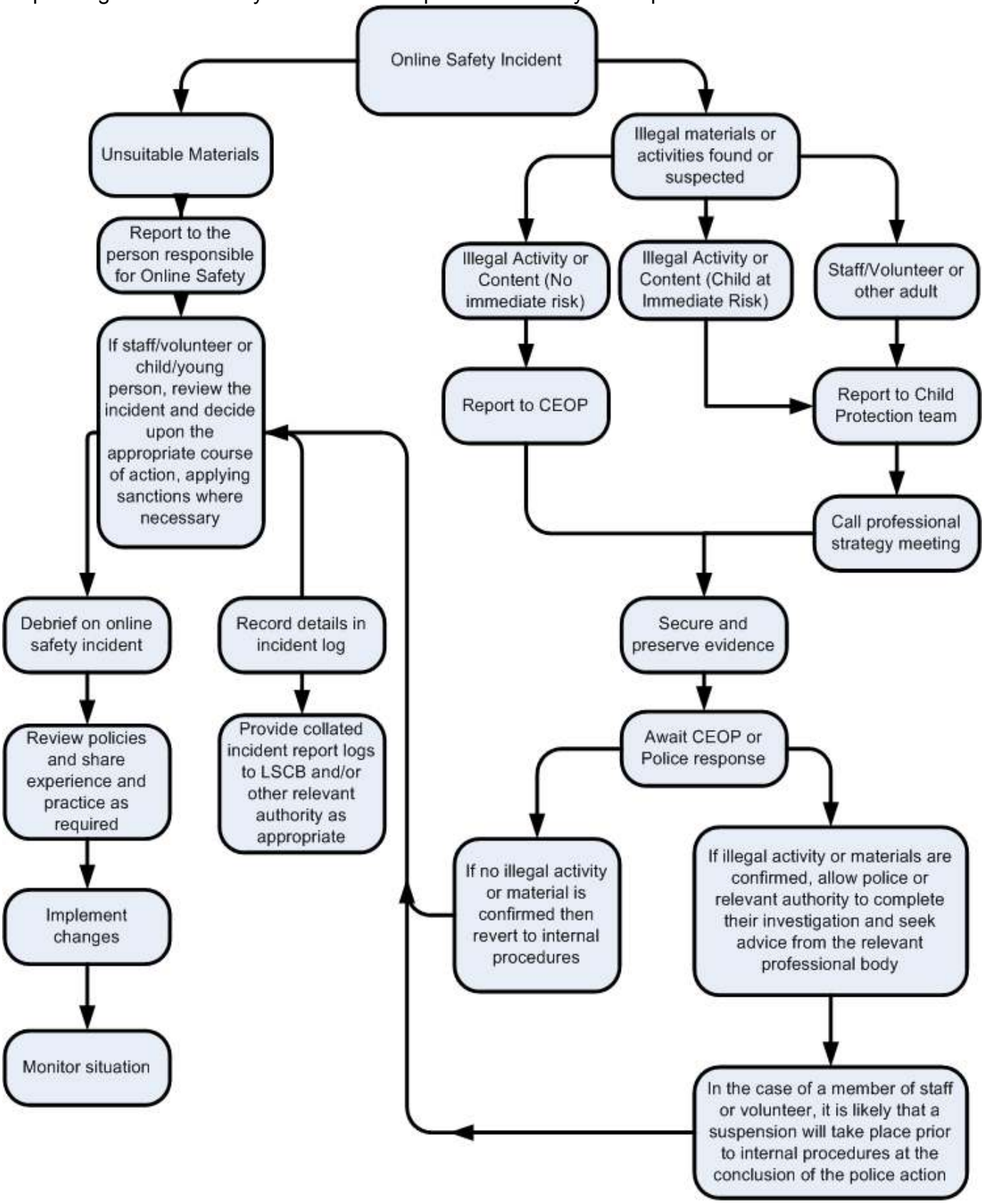
or pass on, material, remarks, proposals or comments that contain or relate to:	**criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986**					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media					X	
Use of messaging apps				X		
Use of video broadcasting eg Youtube				X		

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. This guidance is intended for use when staff need 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 involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

In the event of suspicion, all steps in this procedure should be followed:

- 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 national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and 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.

School / Academy Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Approved by Governing Body:

Signed: ..... (Chair of Governors)