ST JAMES CE JUNIOR SCHOOL

Online Safety Policy

2017 / 2018

Author/Contact Document Path & Filename	Kym Allan KAHSC, A Beattie, S King Staff shared/Policies, Protocols and Procedures	
Document Reference	Online Safety Policy	
Version	02	
Status		
Publication Date	Sept 2017	
Related Policies	This Policy and supporting procedures applies to all who come into contact with children in the School and should be read in conjunction with other related school Policies and procedures notably; Child Protection & Procedures and Code of Conduct for staff & other adults	
Review Date	Sept 2018	
Approved/Ratified by: Name: Position: Signed:	Governing Body	Date:

Please note that the version of this document contained within the Policy Folder on Staff Shared is the only version that is maintained.

Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Version	Date	Comments	Author
01	August 2016	Original document	Sam King
02	August 2017	Updated to include changes in terminology as a result of revised 'Keeping Children Safe in Education' September 2016	Kym Allan, KAHSC

CONTENTS

Definitions

For the purposes of this Policy and procedures a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

Wherever the term 'school' is used this also includes the wrap around care provided by the school – Early Bird and After School Club.

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 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 have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people can 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 Online Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Head teacher 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 individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- 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 Online Safety Policy is used in conjunction with other school policies (e.g. Behaviour, anti-bullying and Child Protection Policies and procedures).

As with all other risks, it is impossible to eliminate risks completely. It is therefore essential, that our focus is on helping children to understand the risks of being online and to become responsible users of technology. Through an ongoing programme of online safety education, we work to build children's resilience to the risks to which they may be exposed, as well as helping them become savvy and risk aware. We hope that this will lead to children becoming effective digital citizens that have the confidence and skills to face and deal with these risks. We ensure that all children

annually understand and agree to our 'Acceptable User Agreement' to ensure they use technology and the internet safely.

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 Online Safety Policy and procedures that follow explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development of this Policy

This Online Safety Policy has been developed by the Head teacher and Mr King

Schedule for Development

The implementation of this Online Safety Policy will be monitored by:	The Head teacher, Mr King
Monitoring will take place at regular intervals:	Annually
The Governing Body / Governors Sub-Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2018
Should a serious online safety incident take place, the following external persons / agencies should be informed:	The Head teacher / outside agencies, e.g.: LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of:
    - Pupils
    - Parents
    - Staff

Scope of the Policy

This Policy applies to all members of the school community (including staff, pupils, volunteers, parents, visitors) who have access to and are users of school ICT systems, both in and out of 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 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 procedures and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the 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 the Governors' Sub Committee 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 Co-ordinator;
- regular monitoring of online safety incident logs;
- regular monitoring of filtering/change control logs;
- reporting to relevant Governors meeting.

Head teacher and Senior Leadership Team

- The Head teacher is responsible 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.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.
- The Head teacher and another member of Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).

Online Safety Co-ordinator

The Online Safety Co-ordinator:

- leads the Online Safety Committee;
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety Policy and procedures/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;
- liaises with school ICT 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 of Governors;
- reports regularly to Senior Leadership Team.

Technical staff – Mr Sam King

The ICT Technician/ICT Co-ordinator is 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 online safety technical requirements outlined in the school's Acceptable Use Agreements and any relevant Local Authority Online Safety Policy and guidance;
- that adults may only access the school's networks through properly enforced password protection procedures, in which passwords are regularly changed;
- that he/she keeps up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator for investigation;
- that monitoring software / systems are implemented and updated as agreed in school Policies.

Teaching and Support Staff

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 procedures;
- they have read, understood and signed the school Staff Acceptable Use Agreement (AUA);
- they report any suspected misuse or problem to the Online Safety Co-ordinator for investigation;
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities;
- pupils understand and follow the school online safety and acceptable use agreement;
- they monitor ICT activity in lessons, extra curricular and extended school activities;
- they are aware of online 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 regarding these devices;
- in lessons, where internet use is pre-planned, pupils are 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 Safeguarding Lead – Mr Andrew Beattie

The Designated Safeguarding Lead (DSL) will be trained in online 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.

Online Safety Committee

Members of the Governor's Committee will assist the Online Safety Co-ordinator with the production / review / monitoring of the school Online Safety Policy and procedures / documents.

Pupils

All pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement, which they are expected to sign before being given access to school systems;
- 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 will also have explained to them the school Policies on the taking / use of images and on the school's stance regarding 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:

Parents 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 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, letters, website / VLE and information about national / local online safety campaigns / literature.

Parents are responsible for:

- endorsing (by signature) the Pupil Acceptable Use Agreement;
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement.

Policy Statements

Education – 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 education will be provided in the following ways:

- A planned online safety programme will be provided as part of ICT / PHSE / other lessons and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages will be reinforced as part of a planned programme of sessions.
- Pupils are 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.
- Rules for use of ICT systems / internet will be posted in all rooms near to the internet devices. Staff and other adults will act as good role models in their use of ICT, the internet and mobile devices.

Education – parents

Many parents 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 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 provide information and awareness to parents through:

- Letters, newsletters, web site, VLE
- Parents evenings
- Reference to the 'SWGfL' Safe website
- Reference to the CEOP Parent Info website - http://parentinfo.org/
- Reference to the Think U know initiative

Education - Extended Schools

Whenever possible, the school will seek to offer family learning courses in ICT, media literacy and online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

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

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and procedures and staff Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at LA information training sessions and by reviewing guidance documents released by the LA and others national organisations e.g. CEOP.
- This Online Safety Policy and procedures and any updates or changes to it will be presented to and discussed by staff in staff meetings.
- The Online Safety Coordinator will provide advice/guidance/training as required to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions. This is particularly important for those who are members of any sub-committee/group involved with ICT/Online safety/Health and Safety/Child Protection. This may be offered in several ways:

- Attendance at training provided by the Local Authority/National Governors Association/ Local Authority or any other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school Senior Leadership Team are responsible for ensuring that the school network is as safe and secure as is reasonably possible and that procedures approved within this Policy are implemented. The team will also ensure that the relevant people named in the above sections are effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the school Security Policy and Acceptable Use Agreements and any relevant Local Authority Online 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 will be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
- All adult users will be provided with a username and password by 'Westcom' who will keep an up to date record of users and their usernames. Users are required to have their password changed every term.
- The "administrator" password for the school ICT system, used by the ICT technician and ICT co-ordinator will be made available to the Head teacher or other nominated senior leader and kept in a secure place.
- Users are 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 CLEO.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to CLEO.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head teacher and Miss Lloyd. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online 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 Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential online safety incident to the Network Manager.
- 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 for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data must never be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum:

Online safety is a focus in all areas of the curriculum and staff will reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use. Procedures are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff must be vigilant in monitoring the content of the websites the pupils visit.

Use of digital and video images – Photographic and 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. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff can take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Images should only be taken using school memory cards, which must not (unless off premises to begin with) be taken off the premises.
- Care must 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, particularly in association with photographs.
- Written permission from parents will be obtained at the beginning of the year, 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.

Following several "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

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 secure password protected devices or files/folders.

Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed, if left in school office	Not allowed
Mobile phones may be brought to school	☒	☐	☐	☐	☐	☐	☐	☒
Use of mobile phones in lessons	☐	☐	☐	☒	☐	☐	☐	☒
Use of mobile phones in social time	☒	☐	☐	☐	☐	☐	☐	☒
Taking photos on mobile phones or other camera devices	☐	☐	☐	☒	☐	☐	☐	☒
Use of hand held devices e.g. PDAs, PSPs	☒	☐	☐	☐	☐	☐	☐	☒
Use of personal email addresses in school, or on school network	☒	☐	☐	☐	☐	☐	☐	☒
Use of school email for personal emails	☐	☒	☐	☐	☐	☐	☐	☒
Use of chat rooms / facilities	☐	☐	☐	☒	☐	☐	☐	☒
Use of instant messaging	☐	☐	☐	☒	☐	☐	☐	☒
Use of social networking sites	☐	☐	☐	☒	☐	☐	☐	☒
Use of blogs	☐	☒	☐	☐	☐	☐	☐	☒

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 Head teacher – in accordance with the staff Code of Conduct, 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 (email, chat, VLE 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 will be provided with individual school email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information must not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities:

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from school and all other ICT systems. Other activities e.g. Cyberbullying is also banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school Senior Leadership Team believes that the activities referred to in the following section are inappropriate in a school context and that users, as defined below, must not engage in these activities in school or outside school when using school equipment or systems. The school Policy restricts certain internet usage as follows:

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 or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					☒
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					☒
	adult material that potentially breaches the Obscene Publications Act in the UK					☒
	criminally racist material in UK					☒
	pornography				☒	
	promotion of any kind of discrimination				☒	
	promotion of racial or religious hatred				☒	
	threatening behaviour, including promotion of physical violence or mental harm				☒	
	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				☒	
Using school systems to run a private business					☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					☒	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				☒	
Creating or propagating computer viruses or other harmful files				☒	
Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
On-line gaming (educational)	☒	☐	☐	☐	
On-line gaming (non-educational)	☐	☐	☐	☒	
On-line gambling	☐	☐	☐	☒	
On-line shopping / commerce	☐	☒	☐	☐	
File sharing	☐	☐	☐	☒	
Use of social networking sites	☐	☐	☐	☒	
Use of video broadcasting e.g. YouTube	☐	☐	☒	☐	

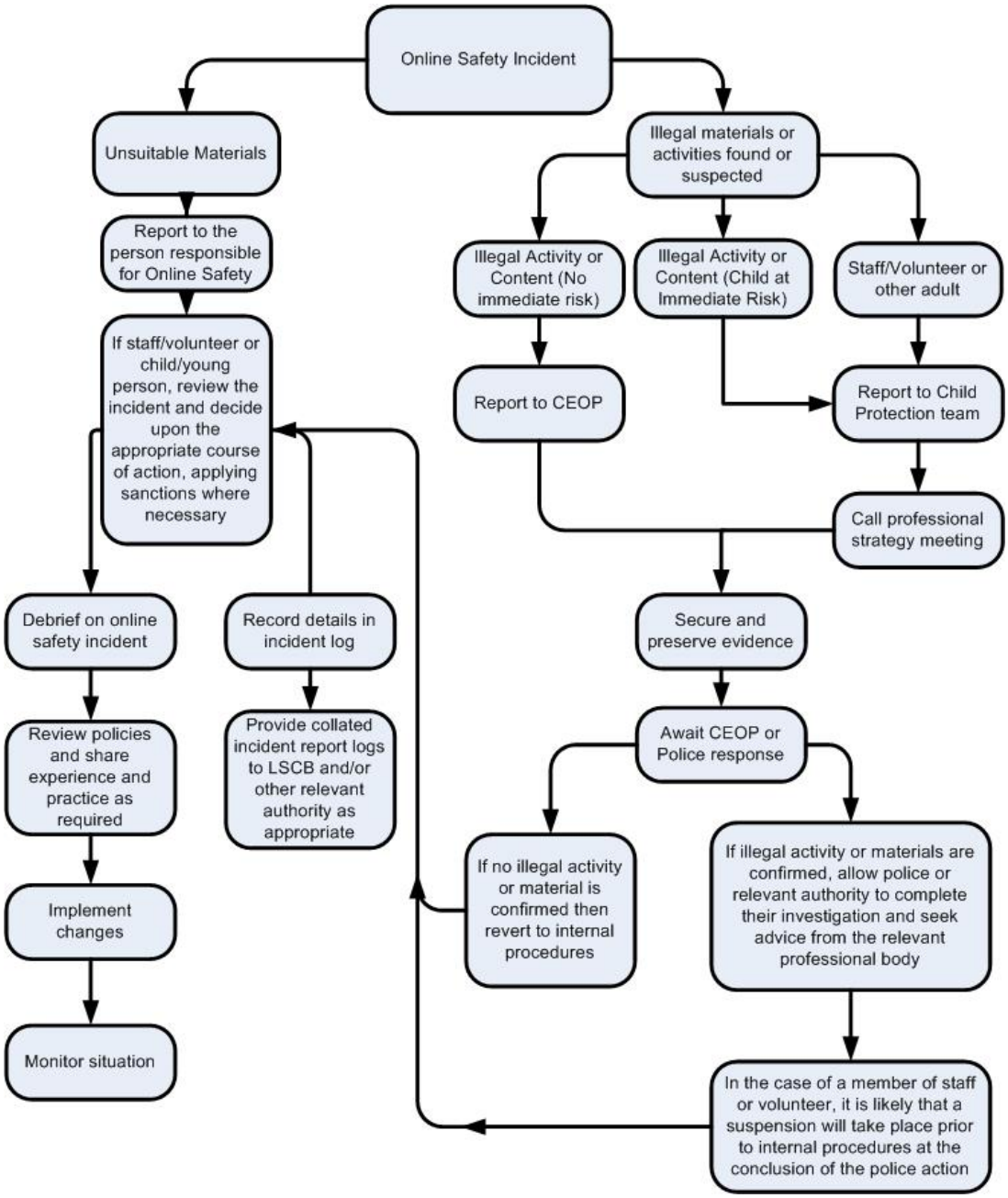
Responding to incidents of misuse:

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this Policy and procedures. However, there may be times when infringements of the Policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials

the flow chart below will be consulted and actions followed in line with the flow chart. In particular, the sections on reporting the incident to the police and the preservation of evidence will be considered.



If a member of staff or another adult suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such an event, the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" will be followed. This procedure and record sheet is replicated at Appendix A. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. In such cases, 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, following investigation, incidents of misuse will be dealt with through the school's behaviour/disciplinary procedures as follows:

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer Senior Manager	Refer to Head teacher	Refer to Police	Refer to technical staff for action re filtering/ security etc.	Inform parents	Removal of network / internet access rights	Warning	Further sanction e.g. detention
Deliberately accessing or trying to access material that could be considered illegal	☒	☒	☒	☒	☒	☒	☒	☐	☐
Unauthorised use of non-educational sites during lessons	☒	☐	☐	☐	☒	☐	☐	☒	☐
Unauthorised use of mobile phone / digital camera / other hand-held device	☒	☒	☒	☐	☐	☒	☐	☒	☒
Unauthorised use of social networking / instant messaging / personal email	☒	☐	☐	☐	☒	☐	☒	☒	☒
Unauthorised downloading or uploading of files	☒	☐	☐	☐	☒	☐	☒	☒	☒
Allowing others to access school network by sharing username and passwords	☒	☐	☐	☐	☐	☐	☒	☒	☒
Attempting to access or accessing the school network, using another pupil's account	☒	☒	☒	☐	☐	☒	☒	☒	☒
Attempting to access or accessing the school network, using the account of a member of staff	☒	☒	☒	☐	☐	☒	☒	☒	☒
Corrupting or destroying the data of other users	☒	☒	☒	☐	☒	☒	☒	☒	☒
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☒	☒	☒	☒	☒	☒	☒	☒	☒
Continued infringements of the above, following previous warnings or sanctions	☐	☐	☒	☐	☐	☒	☒	☐	☐
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☒	☒	☒	☐	☐	☒	☒	☒	☒
Using proxy sites or other means to subvert the school's filtering system	☒	☒	☒	☐	☒	☒	☒	☒	☒
Accidentally accessing offensive or pornographic material and failing to report the incident	☒	☐	☐	☐	☒	☐	☐	☒	☐
Deliberately accessing or trying to access offensive or pornographic material	☒	☒	☒	☒	☒	☒	☒	☒	☒
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☒	☒	☒	☐	☒	☒	☒	☒	☒

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority/HR provider	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	☒	☒	☒	☒	☒	☒	☒	☒
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	☐	☒	☐	☐	☐	☒	☐	☐
Unauthorised downloading or uploading of files	☒	☒	☐	☐	☒	☒	☐	☐
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	☒	☒	☒	☒	☒	☒	☒	☒
Careless use of personal data e.g. holding or transferring data in an insecure manner	☒	☒	☐	☐	☐	☒	☐	☐
Deliberate actions to breach data protection or network security rules	☒	☒	☒	☒	☒	☒	☒	☒
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	☒	☒	☐	☐	☒	☒	☐	☐
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☒	☒	☒	☐	☐	☒	☒	☒
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	☒	☒	☒	☒	☐	☒	☒	☒
Actions which could compromise the staff member's professional standing	☒	☒	☒	☐	☐	☒	☒	☒
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☒	☒	☒	☐	☐	☒	☒	☒
Using proxy sites or other means to subvert the school's filtering system	☒	☒	☐	☐	☒	☒	☐	☐
Accidentally accessing offensive or pornographic material and failing to report the incident	☒	☒	☒	☐	☒	☒	☐	☐
Deliberately accessing or trying to access offensive or pornographic material	☒	☒	☒	☒	☒	☒	☒	☒
Breaching copyright or licensing regulations	☒	☒	☒	☒	☐	☒	☒	☒
Continued infringements of the above, following previous warnings or sanctions	☐	☒	☒	☒	☒	☐	☒	☒

Appendix A

Guidance for Reviewing Internet Sites (for suspected harassment and distress)

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

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

Please follow all steps in this procedure:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the website address 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 senior management 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 disciplinary procedures
    - Involvement by Local Authority or 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
- **Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.**

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

Appendix A

Record of reviewing internet sites (for suspected harassment / distress)

School	St James CE Junior School
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review

Web site(s) address Reason for concern

Conclusion and Action proposed or taken
