Bishop's Waltham Junior School

E-Safety Policy

Policy Background

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 can help 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 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 students / 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 / student 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
- 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 students' / 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.

Policy Development

This e-safety policy has been developed by Jon Senior (ICT subject leader and e-safety co-ordinator), using a model published by the South-West Grid for Learning Trust. It has been reviewed by the Senior Leadership team, the school governors, and the school staff. It has been published on the school website.

(reference - http://www.swgfl.org.uk/Staying-Safe/Content/News-Articles/Creating-an-e-safety-policy--Where-do-you-start-)

It was first written in 2010. It was updated in 2011 to incorporate references to bwjsapps, and in 2012 to incorporate class blogs. It underwent some minor revisions in 2013.

Schedule for Development, Monitoring and Review

Implementation

- An earlier draft of this policy was published in June 2010 after approval from governors.
- It was read by all staff in the Summer Term of 2010, and included in the school's staff new staff induction procedure.
- This draft was written in November 2016. It was reviewed by governors and staff in November 2016 and published on the school website.
- It will be monitored annually, or more often if changes in technology make this appropriate.
- Serious e-safety incidents will be addressed immediately by the e-safety co-ordinator in consultation with the head teacher and any relevant school bodies or appropriate external agencies. The policy will be amended if necessary.

The school will monitor the impact of the policy using

- Logs of reported incidents (maintained by the e-safety co-ordinator).
- Monitoring of the school network where necessary.
- Regular monitoring of the school blog comments and facebook page.
- Monitoring of the school's Google Apps platform where necessary.
- Monitoring of the school's internet access where necessary, and regular reviews of the school's website filtering.
- Parent questionnaires (as used at the end of each academic year).

Roles and Responsibilities

The following section outlines the roles and responsibilities 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* receiving regular information about e-safety incidents and monitoring reports. This information will come from the e-safety co-ordinator via the headteacher. 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 liaison with the E-Safety Co-ordinator / Officer.
- Regular monitoring of e-safety incident logs.
- Reporting to relevant Governors committee / meeting when necessary.

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the 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 / Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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 / Senior Leaders 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 school will need to describe this and may wish to involve the Local Authority in this process).
- The Senior Leadership Team will remain in regular contact with the E-Safety Co-ordinator*.*
- The Headteacher and another member of the Senior Leadership Team 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. These procedures will be outlined within the general Hampshire County Council procedures for allegations against a member of staff.

E-Safety Coordinator / Officer

- 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.
- Provides training and advice for staff.
- Liaises with the Local Authority or other agencies where appropriate and necessary.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets with E-Safety Governor to discuss current issues and review incident logs
- Attends relevant meetings of Governors if appropriate.
- Remains in regular contact with the Senior Leadership Team.

Network Manager & ICT Co-ordinator

The Network Manager and ICT Co-ordinator 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 technical requirements school's Acceptable Use Policy and any relevant Local Authority E-Safety Policy and guidance.
- That users of the school's network (and online learning spaces) gain access using their own usernames and passwords.

- The school’s internet filtering is appropriate and relevant – this will usually tie closely to standard Hampshire settings.
- That they keep 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 and the school’s Google Apps platform is regularly monitored in order that any misuse or attempted misuse can be reported to relevant members of staff, and logged as an e-safety incident

Website (& additional services) manager

The website manager is responsible for ensuring that

- Content loaded to the school website is appropriate, and meets all e-safety guidelines.
- Content loaded to the school blog is appropriate, and meets all e-safety guidelines.
- The links between the school blog, twitter and facebook are working correctly and providing a good service.
- Appropriate e-safety guidelines are followed on our bwjs google apps platform.
- Comments left and approved on the school blog are appropriate, and surnames of children are removed.
- Comments left on the facebook page are dealt with appropriately.
- Staff are trained in the use of class blogs.

Teaching and Support Staff

Teaching 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 Policy / Agreement (AUP).
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation.
- Digital communications with pupils (email / through the blog / bwjsapps / voice) 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, specifically through e-safety work in ICT and PHSE. Pupils understand and follow the school e-safety and acceptable use policy.
- Pupils begin to have an 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.
- They guide children to suitable websites when using the internet, and they understand how to use the processes that are in place for dealing with any unsuitable material that is found in internet searches.
- They provide appropriate guidance to the children in their class about posting to class blogs, and they moderate content as required.

Designated person for child protection / Child Protection Officer

This person 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 or inappropriate materials.

- Inappropriate on-line contact with adults or strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Exposure to websites which foster extremism.

These issues are covered in this policy, the child protection policy, the cyber-bullying policy and the Acceptable Use policy.

(nb. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.)

Pupils

- Are responsible for using the school ICT systems in accordance with the Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Should recognise that material on the internet belongs to the person who originally posted it, and be aware of when it is appropriate to use and share this material.
- 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 and 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 and 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, letters, website / bwjsapps and information about national / local e-safety campaigns / literature where appropriate. Parents and carers will be responsible for:

- Accessing the school website and VLE in accordance with the relevant school Acceptable Use Policy.

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 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 education will be provided in the following ways:

- A planned e-safety programme should be provided as a specific part of the curriculum. This programme will link most clearly to the ICT and PHSE schemes of work, but should be re-inforced in other lessons and 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 in assemblies or other out-of-lesson contexts if appropriate and necessary.
- 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 student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students / 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 and the internet will be posted on a display board in the ICT suite. Condensed versions will be displayed in classrooms.
- 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 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 and carers through:

- The school web site and bwjsapps.
- Other literature or specific events when appropriate.

Education & Training – Staff

It is essential that all staff understand their e-safety responsibilities, as outlined in this policy.

- All staff will read and sign up to the Acceptable Use Policy and the E-Safety policy.
- New staff will read and sign up to these policies as part of their induction.
- Staff will read and regularly review other relevant policies (data protection, child protection, anti-bullying).
- The E-Safety Coordinator will provide advice as required to individuals as required.
- Staff will receive Prevent training in order to be aware of the dangers of radicalisation and extremism online. They will look for signs of radicalisation and report them accordingly.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

- The school, and Hampshire County Council as our provider, will be responsible for ensuring that the school infrastructure and 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.

- Internet filtering, from September 2011, will be delegated to schools. Hampshire will supply a default system which schools can use as a model. As part of this system, certain categories of website will be permanently blocked. Other categories, or specific sites, can be allowed or disallowed by schools. The school will decide what will or will not be allowed.
- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews of the safety and security of school ICT systems.
- Access to the school server is by password only (limited to network manager, headteacher & ICT co-ordinator). The server is not located in a workspace used by children.
- All users will have clearly defined access rights to school ICT systems.
- All network users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames.
- All users of bwjsapps will be provided with a username and password by the googleapps administrator.
- All staff and children will be supplied with usernames and passwords to the school and/or class blog. Children will not be able to post unmoderated content.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).
- Users will be made responsible for the security of their usernames and passwords, 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.
- Any filtering issues should be reported immediately to the ICT co-ordinator.
- Guests to the school (eg trainee teachers) may be given a temporary user name and password by the Network Manager after agreeing to the Acceptable Use Policy. Their account will be closed when it has ceased to be relevant.
- A separate network user name and password is available to supply teachers. This grants them access to the network as a member of staff. Regular supply teachers will have signed up to the Acceptable Use policy.
- As a general rule, staff will not download 'executable' files to the network. On occasions when they do so, they will ensure that such files come from a trusted source. If in doubt, they will consult with the network manager.
- Staff will be responsible for their use of school equipment, particularly with regards to internet usage in school and at home (as described in the Acceptable Use Policy).
- When using removable media (USB sticks, CDs, DVDs), staff will ensure that no undesirable elements are introduced to the school network.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data relating to staff or pupils in the school will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- USB sticks should not be used to store data relating to children due to the dangers of such devices being lost. Their fragile nature also makes them unsuitable for the storage of any data on a long term basis.
- The school runs two wifi networks – one which covers the classrooms, shared areas and other learning spaces, and a smaller (less official) access point in the staffroom. These networks are password protected. Staff are able to sign into the wifi using devices from home (such as mobile phones and tablets) but it is their responsibility to ensure that this log in information is kept private, and that these devices are used in accordance with school policy. Proxy server settings will be needed in order for the devices to connect correctly.

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 students / 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.
- 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.

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 with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission. This includes the downloading and distributing of images from the school blog or bwjsapps.
- 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. Generally, photographs of children on the school website will show children in groups, or shot from an angle which makes the personal identification of children difficult (see the Acceptable Use policy).
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see the Acceptable Use Policy, and the pupil Data Sheets). The website administrator will maintain an up-to-date list of children whose parents have not granted this consent.

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.

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.
- Be fully aware of the risks of transferring data using removable media.

When personal data is stored on any portable computer system, USB stick or any other removable media, it must be securely deleted once its use is complete,

Social Media

The school has no separate and specific policy for social media use amongst staff. We recognise that social media is now an everyday part of life, and it is the responsibility of all staff to engage with social media in a way which will not reflect poorly on the school.

We would recommend that privacy settings on sites such as facebook are kept high, and that references to school activities through personal accounts are kept to a minimum. We would also discourage forming direct links with parents unless they are known to staff in other contexts. Specific information about classes or children, and related photographs, should not be shared in this environment.

Communications

A wide range of rapidly developing communications technologies has 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 with staff permission	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	√ (1)						√(2)	
Use of hand held devices eg PDAs, PSPs	√					√ (3)		
Use of personal email addresses in school, or on school network	√							√
Use of school email and bwjsapps for personal emails	√				√			
Use of chat rooms / facilities		√(4)				√ (5)		
Use of instant messaging	√(6)					√(7)		
Use of social networking sites		√(8)						√(9)
Use of blogs	√ (10)					√ (11)		

(1) Allowed, if the resulting images are handled according the policy statements above.
(2) Allowed, if using school equipment, and with the consent of a member of staff.
(3) Allowed, if relevant to the curriculum.
(4) Most chat rooms will be blocked by our internet filtering, but may be allowed on request as circumstance demands.
(5) Most chat rooms are blocked by our internet filtering, but may be allowed on request as circumstance demands.
(6) Through bwjsapps.
(7) Through bwjsapps.
(8) Social Networking sites are generally by our internet filtering. They can be accessed when necessary so that school accounts can be accessed and maintained.
(9) Social Networking sites are blocked by our internet filtering.
(10) Blogs are covered by the same standards as the rest of our internet usage.
(11) Blogs are covered by the same standards as the rest of our internet usage.

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. The same is true of messages sent through bwjsapps.
- Users need to be aware that email communications and all other activity on bwjsapps may be monitored
- Users must immediately report the receipt of any email or message that makes them feel uncomfortable or is offensive, threatening or bullying in nature. They must not respond to any such email. For children, these incidents should be reported to a teacher, who will follow the appropriate procedures in response, and log the incident with the e-safety co-ordinator (see the Acceptable Use policy and the anti-bullying policy). For staff, these incidents should be reported to the headteacher who will take action as appropriate.
- Any digital communication between staff and pupils or parents / carers (email, chat, googleapps 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 should 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 correctly 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.

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. 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, eg 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 Edict and / or the school					√	
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 (eg 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)		√(1)			
On-line gambling				√	
On-line shopping / commerce		√(2)			
File sharing		√(3)			
Use of social networking sites		√(4)			
Use of video broadcasting eg Youtube		√(5)			

(1) So long as the content of the game is not, in itself, inappropriate.
(2) Allowed by staff, as long as, again, the items purchased are not inappropriate, and such transactions are not carried out in contact time.
(3) So long as this is done in a way which does not contravene network securely (eg, sending a file via e-mail), and no copyright is infringed.
(4) Social networking is blocked by internet filtering by default. If the school allows access to these sites, they will be accessible for staff only.
(5) Some video broadcasting sites may be blocked by our internet filtering. If sites are permitted (through the decisions made as a school), this is allowed as long as the video content is appropriate (and hosted on an appropriate site) and copyright is not breached.

Further details of what is and is not permissible over our school internet connection can be found in our Acceptable Use Policy.

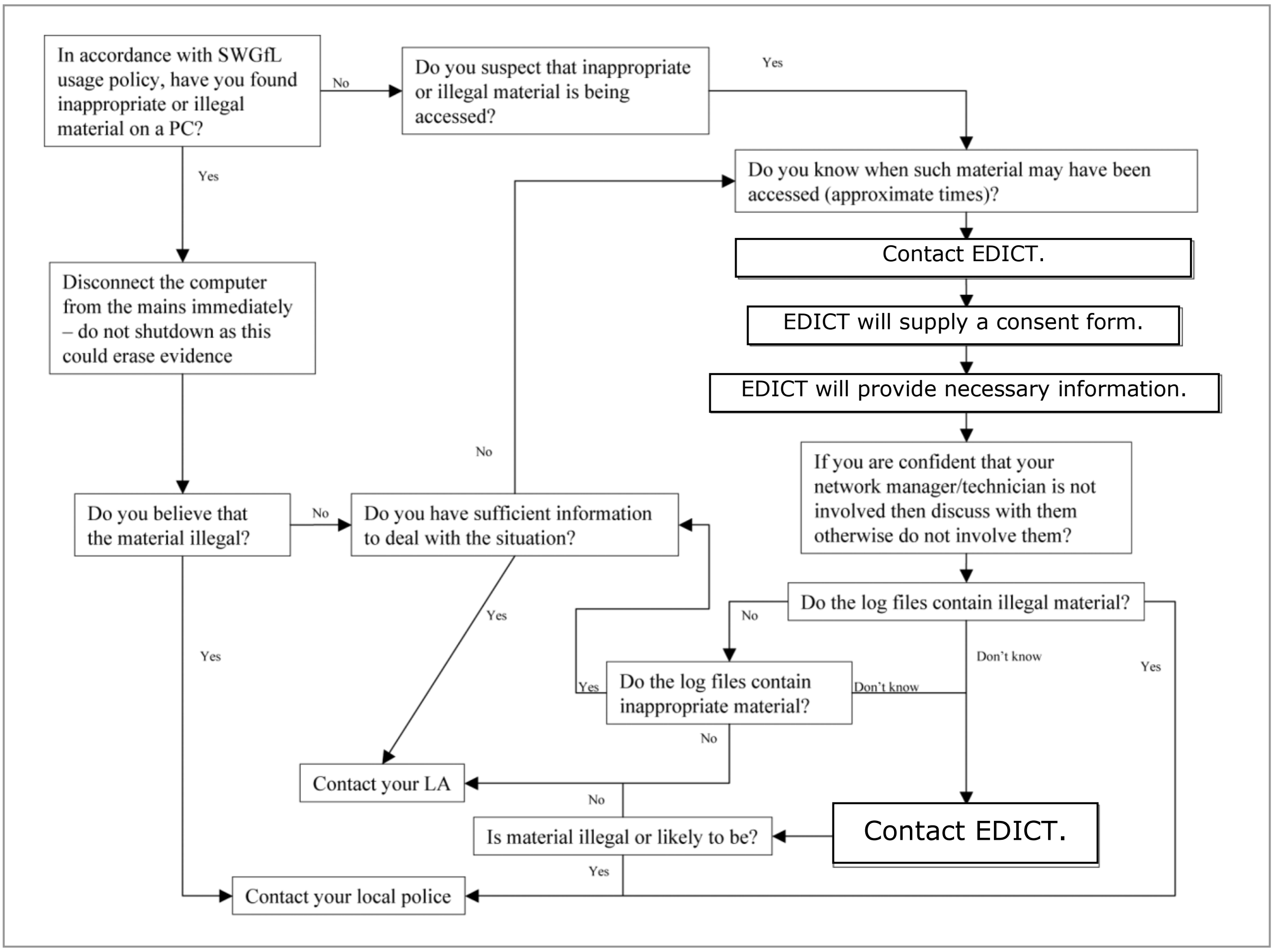
Responding to incidents of misuse

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. 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 ie.

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should 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.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact EDICT.
EDICT will supply a consent form.
EDICT will provide necessary information.
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
No
Yes
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact EDICT.
Yes
Contact your local police

If members of staff 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 event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". 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. 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 as follows:

Pupils								
Incidents:	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		√	√					
Unauthorised use of non-educational sites during lessons	√							
Unauthorised use of mobile phone / digital camera / other handheld 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 student's / 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	√	√		√	√	√		√
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

The following actions would be considered misuse of the schools ICT systems, and could lead to disciplinary action such as a warning, a suspension, referral to the local authority or, in cases of illegality, police 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 eg 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.

The online presence of BWJS

The school website

Our school website is a primary contact point between our school and the outside world. It is used by parents, but also viewed by members of the community, and prospective parents, pupils and staff members. It is important, therefore, that the website is treated well. It should be kept up to date and revised when information is no longer relevant.

Because the website can only be edited through a single point within school, there are very few e-safety issues to consider beyond the following:

- Pupils should not be easily identifiable through the school website. When photographed, children should ideally be in groups, or photographed from an angle that does not clearly show the face. Names may be used, but surnames may not. Parental consent must be granted for a child's image to be on the website.
- Pictures of staff are provided on the website for reference, and they are more identifiable.
- When e-mail address, are used on the website, they must be official school addresses. These will only ever be supplied when permission is granted.
- Sometimes, the school website will include links to external sites. While all of these sites will be initially checked for the suitability of their content, the school cannot be held responsible for any issues caused by following these links. Links should be removed when they are no longer relevant, as the school has no way of ensuring that the content of linked sites does not change.

The school blog

The school blog is our main source of news. It is quicker and easier to update than the main site, and it can be updated by more than one person. All the guidelines applicable to the main website also apply to the school blog. In addition:

- Only authorised users can post material to the blog. All teaching staff will be provided with an identifiable account. They will be classed as 'authors' – able to create their own posts, but not able to edit the posts of others.
- If children are given access to post on the blog, they will be classed as 'contributors' – able to write their own posts, but not able to publish. Their posts will need publishing by an administrator.
- Comments can be left on all blog posts. These will be moderated before appearing publically. During moderation, surnames will be removed from children.
- The blog administrator will retain sole administrator control. They will be responsible for monitoring all blog posts and moderating all comments.
- At times, posters to the blog may choose to embed media created elsewhere – for instance, videos or photo slideshows uploaded to external sites. When this takes place, the creator will ensure that this media is viewable only at the blog.

Class blogs

Each class are provided with their own blog which can be used in whichever way their teacher deems appropriate.

- Only authorised users can post material to the blog. Class teachers are set up as administrators on their class blogs (as is the ICT co-ordinator). They are able to post to their blog and edit posts and comments left by others. They are also able to remove content. Children are classed as 'contributors' – able to write their own posts, but not able to publish. Their posts will need publishing by an administrator. They are not able to post pictures to the blog unless their role is changed – their class teacher is able to temporarily change user's roles if they wish.

- Comments can be left on all blog posts. These will be moderated before appearing publically. During moderation, surnames will be removed from children.

Twitter and Facebook

The school blog is automatically exported to a dedicated twitter feed. This, in turn, is fed to a facebook page. Both these services allow people to follow the news from the blog in a different environment. These services are entirely automated.

- The website manager will keep both services under review.
- On facebook, posting rights are disabled to users. Only specifically authorised 'administrators' are able to post to the page. Users can leave comments – these comments will be regularly monitored and removed if necessary.
- Content published to both services is very limited – just a headline and a link back to the blog. Photographs will never be published to either site.
- Followers of both services can be blocked if necessary.

We have created these services because we recognise their value in communicating with parents and other interested parties. As a school, however, we recognise that neither of these services should be used by children. Both twitter and facebook have a minimum user age of 13, and while we realise that many children circumvent these rules to have an account at one site or the other, we will block them from following the school.

Bwjsapps.co.uk

Our google apps platform will be accessible to all staff and children at the school. Each user will have their own username and password. Children will be taught how to use the service during ICT times, but the service will also be available as a tool for teaching the curriculum as a whole, and at home if users wish to use it.

Users will need to be taught the following e-safety points which they will be responsible for remembering:

- Activity on bwjsapps will be monitored, and access rights can be withdrawn if rules are broken.
- Children will be responsible for learning and remembering their usernames and passwords.
- Bwjsapps e-mail is to be used sensibly and appropriately. It does not need to be limited to 'curriculum' use, but it must be used politely. Children should not send bulk messages to large lists of people without reason, and they must not ever use e-mail to upset, harass or bully other users.
- Material created at bwjsapps may be viewable to other users, but it will not be viewable to people outside the system.
- Messages in and out of the system will be blocked for children – they can neither send or receive messages to addresses that do not end in bwjsapps.co.uk unless they have been granted specific access to be able to do so. This access will only be provided for specific domains if the curriculum requires it – it will then be withdrawn.