St John's Catholic Primary School
BATH

'For everyone to shine, celebrate and grow'

Email: stjohnsbath_pri@bathnes.gov.uk
Website: www.stjohnscatholicprimary.org.uk
Head Teacher: Mrs A Bennett

E-Safety and Social Networking Policy 2018/19

1.0 Rationale

New technologies are an integral part of our lives and are powerful tools, which open up teaching and learning opportunities for pupils and schools' staff in many ways. This document aims to:

- Assist pupils and schools' staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to internet usage and social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Prevent adults abusing or misusing their position of trust
- Prevent children or staff suffering from cyber-bullying
- Provide a clear procedure for reporting any incidents

2.0 Overview

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, 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 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 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.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their Head teachers of the justification for any such action already taken or proposed. Head teachers will in turn seek advice from the Schools' HR team where appropriate.

Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct that would lead any reasonable person to question their motivation and intentions. They should work and be seen to work, in an open and transparent way. They should also continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Social Media Definition
For the purpose of this policy, social media is the term commonly used for websites that allow people to interact with each other in some way – by sharing information, opinions,

knowledge and interests. Social networking websites such as Facebook, Twitter and Instagram are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and communication apps such as Whatsapp. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day. It also applies to the use of communication technologies such as mobile phones, cameras, iPads, iPods, tablets or other handheld devices and any other emerging forms of communications technologies.

3.0 Roles and Responsibilities

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

3.1 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. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- delegate a governor to act as E-Safety link
- E-Safety Governor works with the E-Safety Leader to carry out regular monitoring and report to Governors
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting
- approve and review the effectiveness of the e-safety Policy

3.2 Head teacher and Senior Leaders

- The Head teacher 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 Head teacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head teacher and another member of the Senior Management 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.

3.3 E-Safety Coordinator

- 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
- Liases with the Local Authority

- Liases with school ICT technical staff
- 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
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Management Team

3.4 Child Protection Officers

Child Protection Officers 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

3.5 Technical staff

Systems Managers / ICT Technicians 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 and any relevant Local Authority E-Safety Policy and guidance
- 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 the 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 / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Head teacher for investigation / action / sanction

3.6 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 Policy (AUP)
- they report any suspected misuse or problems to the E-Safety Co-ordinator / Head teacher for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / 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
- 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

3.7 Pupils

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (For EYFS & KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- 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

3.8 Parents / Carers

The school will take every opportunity to help parents understand e-safety issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

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

3.9 Community Users

Community Users who access school ICT systems / website / Merlin as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

4.0 Policy Guidelines

4.1 Education of pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and PSHE activities
- Pupils will be advised never to give out personal details of any kind that may identify them, their friends or their location.
- All pupils will be provided with an individual login for educational use.
- 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.
- The school will ensure that there is no access to social networking sites, and will consider how to educate pupils in their safe use.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils should be taught in all lessons to be critically aware of what they access on-line and be guided to check the accuracy of information
- Rules for use of ICT systems / internet will be taught to the children and displayed in all rooms
- Video conferencing should use the schools broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing and webcam use will be appropriately supervised for the pupil's age.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

4.2 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.
- Pupils should be taught in all lessons to be critically aware of the information they access on-line and be taught to check 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.

4.3 Education of parents / carers

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

- Letters, newsletters, web site.
- Parents evenings with class teacher
- E-Safety open evening with parents

4.4 Training of Staff

All staff will receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A staff meeting covering safety training annually for teaching staff to ensure that they fully understand the school e-safety policy and Acceptable Use Policies. This training will also repeated with support staff.
- All new staff should receive e-safety, child protection and safer working policy training as part of their induction programme.
- The E-Safety Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

4.5 Training of 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 will be offered in a number of ways:

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

4.6 Technical Guidelines (infrastructure / equipment, filtering and monitoring)

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that 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:

- Our school ICT system will be managed in a way that ensures that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy 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 (staff and children) will be provided with a username and password. Staff will be required to change their password each year.
- The "administrator" password for the school ICT system, used by the Network Technicians must also be available to the E-safety Co-ordinator 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
- In the event of the Network Technician 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.
- 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 Network Manager and Head teacher. 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 email communication, and users are made aware of this in the Acceptable Use Policy.
- Any actual / potential e-safety incident must be reported immediately to the E-safety coordinator and Head teacher who will then inform the Network Manager.
- There is a provision of temporary access of "guests" (eg trainee teachers, supply teachers) onto the school system with individual logins issued to staff that are working at the school for a term or more.
- Staff are made aware that rules regarding the installation of programs and use of removable media (eg memory sticks / CDs / DVDs) apply to portable devices at school and home.
- 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.

4.7 Protection of data

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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

4.8 Protection of personal information

Adults working in schools should:

- Never share their work log-ins or passwords with other people.
- Keep their personal phone numbers private
- Not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used.
- Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.
- Keep their mobile phones securely away from pupils to ensure that no child gains access to them.
- Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

4.9 Use of digital and video images - Photographic, Video

Working with children may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of children. Staff and pupils will be made aware of the risks associated with sharing images and with posting digital images on the Internet:

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or appearing in the press (General Consent Form will be completed by parents or carers when their child starts school).
- Where possible, permission from the child should always be sought before an image is taken for any purpose.
- Staff are allowed to take digital / video images to support educational aims, but those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- It is not appropriate for adults to take photographs of children for their personal use.

- Staff mobile phones must only be used to take photographs of children if the staff member considers it absolutely necessary i.e. at a sporting event where the member of staff has no school camera. The staff member has a duty to ensure that the photos are deleted immediately after the event. This process must be completed in the presence of another member of staff.
- The images taken will only be stored on the school system, accessible to teaching staff and will be destroyed once the child has left the school.
- 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
- 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 they will recognise the risks attached to publishing their own images on the Internet eg on social networking sites.
- 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 or blog, particularly in association with photographs.

4.10 Use of Communication Technology within school

The following table shows how staff and pupils can use communication technologies within school:

	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	✓				✓ but kept in the office			
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 eg iPads, iPods, tablets		✓						✓
Use of personal email addresses 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		✓					✓	

The school ICT systems are primarily used for educational use. Occasional and reasonable private use is permitted provided that this does not interfere with the performance of the user's, or another user's, duties. Private use is also subject to the same rules and controls that govern business use. Access should only be undertaken in the user's own time.

4.11 Acceptable use of the Internet

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 SWGfL 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					☐	
On-line shopping / commerce			☐			
File sharing i.e on SharePoint or One Drive			☐			

4.12 Safer online behaviour – Social Networking Sites

- Managing personal information effectively makes it far less likely that information will be misused.
- In their own interests, adults within school settings need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or

friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

- All adults, particularly those new to the school setting, should review their social networking sites regularly to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.
- Adults should never make a 'friend' of a pupil or ex-pupil at the school, where they are working, on their social networking page.
- Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and staff need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.
- Staff need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Bath and North East Somerset Council could result in formal action being taken against them.
- Adults are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.
- Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or Bath or North East Somerset Council into disrepute or could reflect negatively on their professionalism.
- Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher/teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the Local Authority.

4.13 Access to inappropriate images and Internet usage

- There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and disciplinary action being taken.
- Adults should not use equipment belonging to their school to access any adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.
- Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools need to ensure that Internet equipment used by pupils have the appropriate controls with regards to access e.g. personal passwords should be kept confidential.
- Where indecent images of children are found, the police and local authority designated officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against adults policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.
- Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the LADO should be informed and advice sought. Schools should refer to the dealing with allegations of abuse against adults policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

4.14 Communication between pupils or parents / adults working in school

- Communication between pupils and adults by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.
- Any digital communication between staff and pupils or parents (email, chat, VLE etc) must be professional in tone and content.
- Adults should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.
- The school provides a work mobile (of which there are 6) for communication between staff and parents where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers to parents for these purposes.
- The school provides a work email address for all staff. The official school email service may be regarded as safe and secure and is monitored. Staff and pupils or parents should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.
- Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour that could be construed as 'grooming' in the context of sexual offending.
- E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.
- Users must immediately report, to the E-safety coordinator and Head teacher, 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.

4.15 Social contact

- Adults should not establish or seek to establish social contact via social media / other communication technologies with pupils or their families.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Head teacher where there may be implications for the adult and their position within the school setting.
- If a child or parents seeks to establish social contact, or if this occurs coincidently, the adult should exercise her/his professional judgement in making a response but should always discuss this with the Head teacher or the parent of the child.
- There must be awareness on the part of those working with or in contact with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the adult's own family.

4.16 Cyber bullying

- Cyber bullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

- Prevention activities are key to ensuring that adults are protected from the potential threat of cyber bullying. All adults are reminded of the need to protect themselves from the potential threat of cyber bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.
- If cyber bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.
- Adults may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process. Employees will also have access to the BUPA Employee Assistance 0800 269 616, a free confidential counselling and advisory service subject to funding being agreed.
- Adults are encouraged to report all incidents of cyber bullying to their phase leader or the Head teacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.
- Children should be made aware of the potential threat of cyber bullying and the steps that they can take to prevent it (e.g. not sharing their personal information online). They should also be taught what to do if cyber bullying does take place, as part of their ongoing e-safety training.
- Any incidents of cyber bullying should be reported to the E-Safety Co-ordinator and Head teacher. All such incidents will be dealt with in accordance with the school's Anti-Bullying policy.

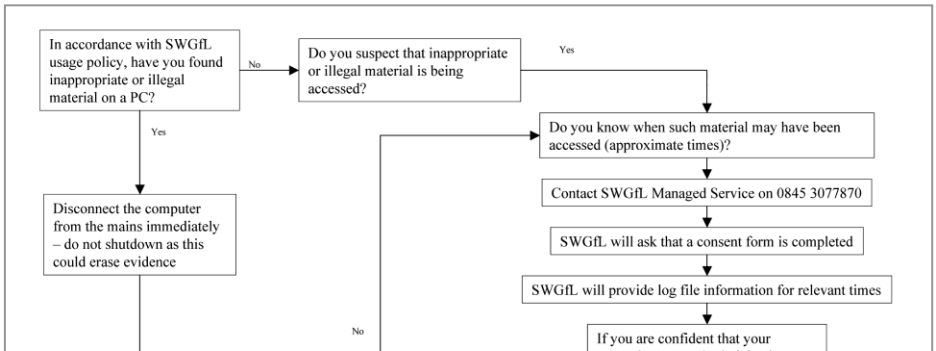
5.0 Procedures for responding to incidents of misuse

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
- evidence of any other hate crime, criminal conduct, activity or materials

the flow chart below 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.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, 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:

5.1 Procedure for pupils

Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to E-safety coordinator	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	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	☐	☐	☐			☐	☐		☐
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	☐	☐	☐	☐	☐	☐	☐	☐	☐

5.2 Procedure for staff

Staff Actions / Sanctions

Incidents:	Refer to E-safety coordinator	Refer to Headteacher	Refer to Local Authority / HR	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	☐	☐			☐			☐
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 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	☐	☐	☐	☐	☐		☐	☐
Continued infringements of the above, following previous warnings or sanctions		☐	☐				☐	☐

6.0 Review of policy

Due to the ever changing nature of information and communication technologies it is best practice that this policy be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing	

Body / Governors Sub Committee on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator, ICT coordinator, Senior Leadership Team, ICT link Governor
Monitoring will take place at regular intervals:	Termly
The Governing Body / Governors Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually or as incidents occur
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 anticipated review date will be:	June 2018
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of pupils, parents / carers, and staff