Kingsmead	**POLICY TITLE:**	**ICT & Online Safety Policy** **(inclusive of password and filtering security)**
Committee/Person Responsible for Policy:		Deputy Headteacher Student Achievement and Teaching & Learning Achievement, Teaching & Learning Sub-Committee
Date Approved by Governing Body:		July 2017
Date of Last Review:		Term 6 2016/17
Next Review Due:		Term 6 2017/18
Associated Documents		Safeguarding and Child Protection; Staff & Volunteer Acceptable Use; Student & Parent/Carer Acceptable Use

The ICT & Online Safety Policy is rooted in the Core Values of Kingsmead School

1) Care
   The Online Safety of student's need(s) is always the driving factor when using ICT

2) Aspiration
   The core purpose of any school is to enable students' highest possible achievement and attainment through powerful learning. ICT provides access for the student to that learning that is in accordance to the "ICT for Learning" vision of dynamic, accessible and personal

3) Respect
   Students should use ICT in a respectful and positive manner

4) Determination
   ICT should be used to enhance the outcomes of the learners in line with their willingness to succeed

Contents

School Policy

New technologies have become an integral part of our lives. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and enhance learning in all areas of the curriculum.

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. Kingsmead School Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy will 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 themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote 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 Online Safety policy is used in conjunction with our other school 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' 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.

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

Development/ Monitoring/ Review of this Policy

This Online Safety policy was approved by the Governors Sub Committee in:	June 2017
The implementation of this Online Safety policy will be monitored by the:	Governors Sub Committee - (Curriculum & Achievement) this is the Online Safety Working Group
The Governors Sub Committee - (Curriculum & Achievement) will receive a report on the implementation of the Online Safety policy generated by the ICT Service Team (which will include anonymous details of Online Safety incidents) at the following intervals:	Termly meetings
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:	June 2018
Should serious Online Safety incidents take place, the following persons should be informed:	Mr M Williams (DHT & Online Safety Officer) Mr P Hopkins (Leader of ICT Services) Mr M Griffin (Headteacher)

The school will monitor the impact of the policy using:

- Records of reported incidents
- Lightspeed Rocket monitoring logs of internet activity – Filtering Lists
- Internal monitoring data for network & email activity – Office 365 tools
- Surveys / questionnaires of
    - Students
    - Parents / carers
    - Staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 will, where known, inform parents/ carers 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 – (Curriculum & Achievement) receiving information about Online Safety incidents and monitoring reports. The chair of the governors' sub-committee responsible for (Curriculum & Achievement) will take on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the Online Safety Co-ordinator/ Officer
- Monitoring of Online Safety incidents
- Reporting to full Governors

These activities may take place in an electronic format to allow quicker, more effective action to be taken if necessary.

Headteacher and Senior Leadership Team:

The Headteacher 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 – Mark Williams (DHT)

- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant
- The Senior Leadership Team will receive monitoring reports from the Online Safety Coordinator/ Officer. This will take place through SLT meetings and when and where necessary to cover more serious matters.
- The Headteacher and the Business Manager should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online Safety Officer:

- Brings updates to the Governors Sub Committee – (Curriculum & Achievement)
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/ 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 school ICT technical staff
- receives reports of Online Safety incidents
- meets with Online Safety Governor to discuss current issues, review incidents
- attends relevant meeting/ committee of Governors
- Reports to Senior Leadership Team

ICT Services Leader/ Technical Staff:

The Leader of ICT Services 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
- That users may only access the school's networks through a properly enforced password protection policy

- Schools Broadband is informed of issues relating to the filtering structure
- that he keeps up to date with Online Safety technical information in order to effectively carry out his 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 Coordinator
- That monitoring software/ systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current school Online 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 Online Safety Coordinator for investigation/ action/ sanction
- Digital communications with students/ (email/ Firefly Kingsmead Virtual Learning Environment (VLE) should be on a professional level
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school Online Safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular 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 with regard to these devices

Designated person for child protection/ Child Protection Officer

Should 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

The designated Online Safety Officer has the following powers in respect of child protection

The Online Safety Officer is allowed to access sites or workspaces owned by students (Facebook etc.) where a significant child safety risk is posed. In all cases parents/carers should be contacted but if permission for access is refused then the school still retains the right to this access if the Child Protection officer, the Online Safety Officer and the Headteacher/ Senior officer present in school on that day agree.

As the technical knowledge of parents grows, it is important that schools offer the most interactive way of reaching parents. Therefore the designated Online Safety officer may also operate Online Safety information bulletins on services such as Twitter or Facebook. The Online Safety officer has to share access to these accounts with a senior leader and the designated Child Protection officer to ensure their own Online Safety.

Online Safety Committee

Members of the Online Safety committee will assist the Online Safety Coordinator with:

- The production/ review/ monitoring of the school Online Safety policy/ documents.
- The assistance in monitoring information services to parents such as Facebook and Twitter.

Students:
- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 BYOD i.e. 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 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/ Carers
Parents/ Carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/ Firefly Kingsmead VLE and information about national/ local Online Safety campaigns/ literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- Accessing the school website/ VLE/ on-line student records in accordance with the relevant school Acceptable Use Policy.

Community Users
Community Users who access school ICT systems/ website/ Firefly Kingsmead VLE as part of the Extended School provision will be expected to sign the staff AUP before being provided with access to school systems.

Policy Statements

Education – students
Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 the Programme of Study in ICT – 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 assemblies.
- Students 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

- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/ internet will be posted in all rooms and displayed on log-on screens of both students and staff.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/ carers

Many parents and carers may only have 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.

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

- Letters, newsletters, web site, Firefly Kingsmead VLE
- Parents evenings
- Reference to a number of online safety websites in the AUP for Parents and Students.

Education & Training – Staff

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

- Online Safety training will be made available to all staff. It is expected that some staff will identify Online Safety as a training need within the performance management process. Online Safety training will take the form of INSET, online activities, staff meetings, department meetings etc.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies. This will be carried out through the induction meetings that new staff receive. In addition to this the school offers this training to all trainee teachers and assistants who work at the school, whether temporary or permanent.
- The Online Safety Coordinator will receive updates through attendance at training sessions and by reviewing guidance documents.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/ team meetings/ INSET days.
- The Online Safety Coordinator will provide advice/ guidance/ training to individuals as required.

Training – Governors

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

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

Technical – 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 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 Online Safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements
- 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 where possible
- All users will have clearly defined access rights to school ICT systems through group policy. Users can be made aware of their own group policy access rights at any time by contacting the ICT department, although any requested changes to these access rights is solely at the discretion of the Leader of ICT services/ Online Safety Officer. Any changes must comply with this online safety policy and the AUP of the requesting individual.
- All users will be provided with a username and password by the Leader of ICT Services who will keep an up to date record of users and their usernames.
- The "master/ administrator" passwords for the school ICT system, used by the Leader of ICT Services (or other person) must also be available to the Headteacher or Online Safety Officer and kept in a secure place (e.g. 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.
- Users are advised to change their password annually. That the password should be a minimum of 8 characters and should include uppercase characters, lower case characters, numbers and special characters. The password should not include proper names.
- The school maintains and supports the managed filtering service provided by School Broadband - LightSpeed
- In the event of the Leader of ICT Services (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 Online Safety Officer.
- Any filtering issues should be reported immediately to Schools Broadband.
- Requests from staff for sites to be removed from the filtered list will be considered by the Leader of ICT Services and Online Safety Officer. If the request is agreed, this action will be recorded and reviewed 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 Policy. Microsoft monitoring tools are used to enable this process both by teachers of classes and the ICT department
- Actual/ potential Online Safety incidents are reported directly to the Leader of ICT Services or Online Safety Officer.
- 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 policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. All temporary staff must sign the staff AUP and be made aware of this Online Safety policy
- An agreed policy is in place through the AUP's regarding the downloading of executable files by users
- An agreed policy is in place through the AUP's regarding the extent of personal use that users (staff/ students/ community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (*see Appendix 4*)
- An agreed policy is in place through the AUP's that allows staff to/ forbids staff from installing programmes on school workstations/ portable devices.
- An agreed policy is in place through the AUP's regarding the use of removable media (e.g. memory sticks/ CDs/ DVDs) by users on school workstations/ portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software. (Sophos)
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should 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 students 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 students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Leader of ICT Services temporarily remove those sites from the filtered list for the period of study.
- Students 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
- Students 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 students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students 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 students 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 e.g. 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' 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 students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.

Sexting – Youth Produced Sexual Imagery

What is sexting?

- Sexting involves creating, sending, receiving, possessing or forwarding 'sexts'.
- 'Sexts' is a colloquial term that describes sexually explicit SMS or MMS, emails, photos, videos; as well as posts or blogs on social networking websites like Facebook, Myspace or Twitter, or images or clips from Skype.
- 'Sexually explicit' is content that by society's standards is "sexually offensive" e.g. nude or semi-nude images, material depicting persons engaging in sexual activity or in sexually suggestive poses.

The Law

Children who are 'sexting' may actually be committing criminal offences.

Crimes involving child abuse images fall under Section 1 of the Protection of Children Act 1978. This Act was amended by the Sexual Offences Act 2003 to extend the definition of children from under 16's to under 18's.

It is a crime to take, make, permit to take, distribute, show, possess, possess with intent to distribute or to advertise indecent photographs of any person below the age of 18 years.

If someone is prosecuted for these offences, they may be placed on the sex offenders register, potentially for some considerable time.

If staff become aware of a student's involvement in 'sexting' the procedure in Appendix 3 will be implemented.

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.
- 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 be checked using an approved virus checker before any data is stored on it.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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

	Staff & other adults				Students			
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 (With Permission from Head Teacher)		*					*	
Use of hand held devices	*					*		
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. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/ carers (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.

- All students will be provided with individual school email addresses for educational use.
- Students 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 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, 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					*	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LightSpeed 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 (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 (using p2p networks such as U Torrent)				*	
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. 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:

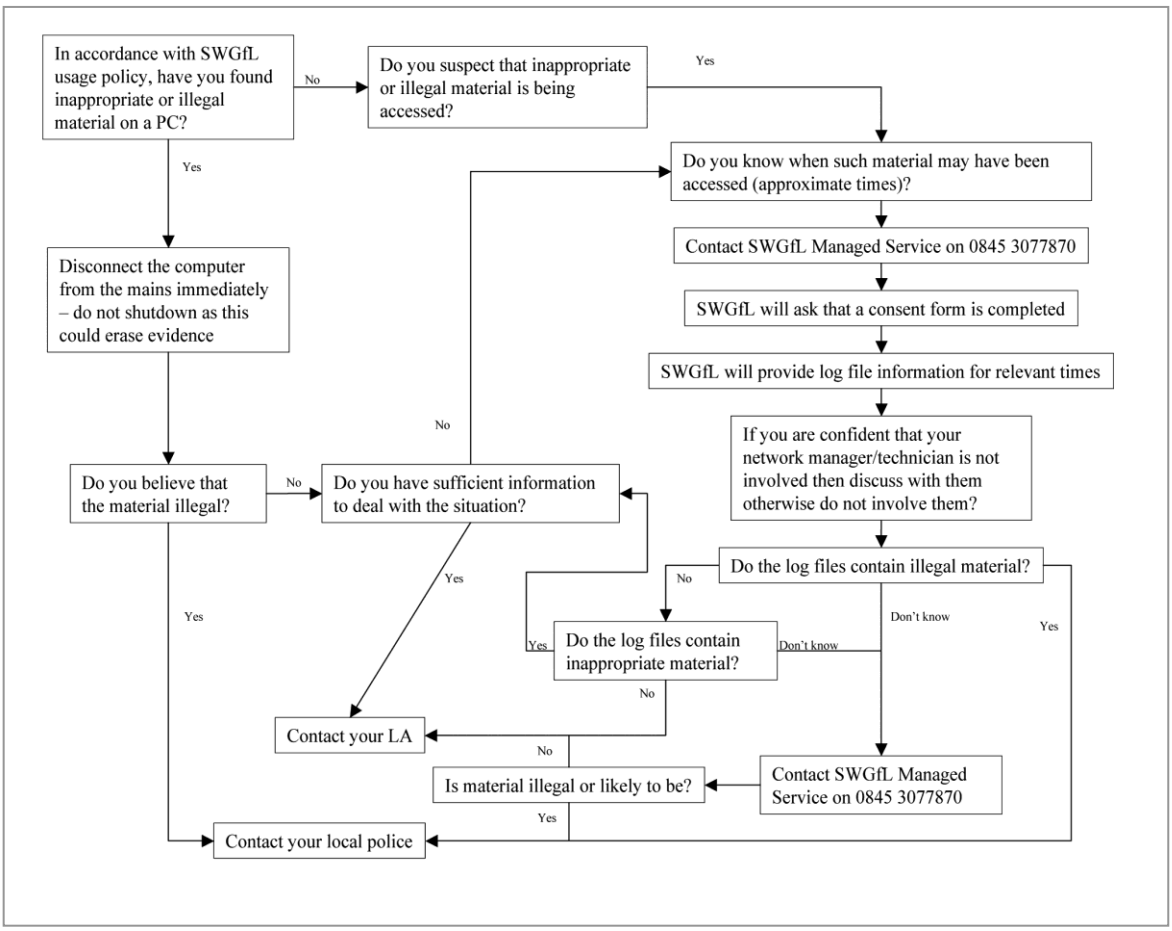
If any apparent or actual misuse appears to involve illegal activity i.e.:

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

The Headteacher or Online Safety Manager should be contacted prior to following the flow chart (From SWGfL) – below, unless you suspect them of involvement, in which case another member of SLT should be consulted. http://www.swgfl.org.uk/safety/default.asp should also

be accessed for further guidance on actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Equally the school will follow the policies laid out in the Child Protection documentation and will inform necessary member of staff immediately to ensure the safeguarding of our young people.



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. 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:

These tables indicate the level of authority approached in the first instance and the likely action to be taken. Clearly both should escalate if the offence is repeated.

Students **Actions/ Sanctions**

Incidents:	Dealt with by class teacher/ tutor	Dealt with by Head of Department or Head of Year	Dealt with by Online Safety Manager or Headteacher	Refer to Police	Refer to technical support staff for action re filtering/ security etc.	Inform parents/ carers	Removal of network/ internet access rights	Other internal sanctions	Further sanction e.g. 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 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	*	*			*	*		*	*
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 **Action/ Sanctions**

Incidents:	Dealt with by line manager or E Safety Manager	Dealt with by Head teacher	Dealt with by Governors	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	*	*			*			
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	*							

Appendices

- Blogging Acceptable Use Policy
- Use of ICT – Practical advice for teachers
- Sexting in school – Response process for professionals

Appendix 1 **Blogging Acceptable Use Policy**

Before starting your blog - please read the following 'Blogging Acceptable Use Policy':

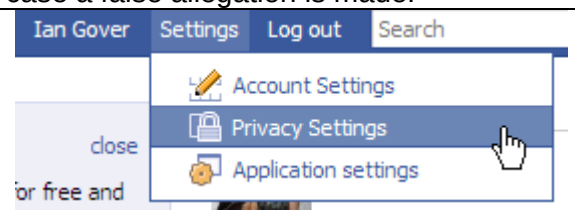
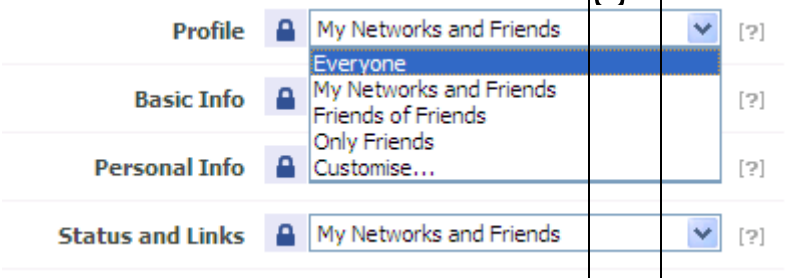
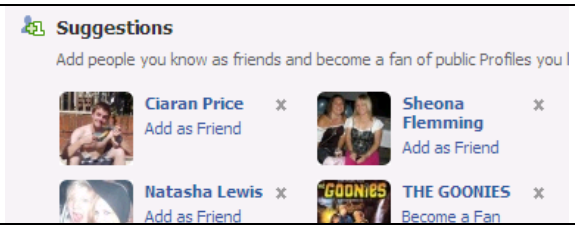
The most basic guideline to remember when blogging is that the blog is an extension of your classroom. You should not write anything on a blog that you would not say or write in your classroom. Use common sense, but if you are ever in doubt ask a teacher or parent whether or not what you are considering posting is appropriate. If you are going to err, err on the safe side. Here are some specific items to consider:

1. The use of blogs is considered an extension of your classroom. Therefore, any speech that is considered inappropriate in the classroom is inappropriate on a blog. This includes, but is not limited to, profanity; racist, sexist or discriminatory remarks; personal attacks.
2. Blogs are used primarily as learning tools, either as extensions of conversations and thinking outside of regular class time, or as the basis for beginning new classroom discussions. Either way, be sure to follow all rules and suggestions that are offered by your teachers regarding appropriate posting in your class.
3. Blogs are about ideas – therefore, agree or disagree with the idea, not the person. Freedom of speech does not give you the right to be uncivil. Use constructive criticism and use evidence to support your position. Read others' posts carefully – often in the heat of the moment you may think that a person is saying one thing, when really they are not.
4. Try not to generalize. Sentences that start with words like "All" (e.g., "All teachers," "All administrators," "All liberals," "All conservatives") are typically going to be too general.
5. Blogs are public. Whatever you post on a blog can be read by anyone and everyone on the Internet. Even if you delete a post or comment, it has often already been archived elsewhere on the web. Do not post anything that you wouldn't want your parents, your best friend, your worst enemy, or a future employer to read.
6. Blog safely. NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). (Note: The advice to not use your last name is for your protection. Teachers may choose to use their last names for their posts/comments.) Do not, under any circumstances, agree to meet someone you have met over the Internet.
7. Because your login to the blogging site (e.g., Blogger) is typically linked to your profile, any personal blog you create in class is directly linked to your class blog and must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in your profile or in any posts/comments you make), you need to realise that anywhere you use that login links back to your class blog. Therefore, **anywhere** that you use that login (posting to a separate personal blog, commenting on someone else's blog, etc.), you need to treat the same as a school blog and follow these guidelines. You should also monitor any comments you receive on your personal blog and - if they are inappropriate - delete them. If you would like to post or comment somewhere and not follow these guidelines, you need to create a separate login to the blogging site so that it does not connect back to your class blog. You may **not** use that login from school computers. We would still recommend you follow the portion of these guidelines that address your personal safety (e.g., not posting personal information, etc.)
8. Linking to web sites from your blog or blog comments in support of your argument is an excellent idea. But never link to something without reading the entire article to make sure it is appropriate for a school setting.
9. Use of quotations in a blog is acceptable. Make sure that you follow the proper formatting and cite the source of the quote.

10. Pictures may be inserted into a blog. Make sure that the image is appropriate for use in a school document and copyright laws are followed. Do not post any images that can identify yourself or others

Appendix 2 **Practical ICT Advice for Teachers**

No-one else should use your laptop	If another member of the family is allowed to use the school provided computer it is difficult to ensure that the use is appropriate. If there is inappropriate material on a laptop then the person who is allocated that computer is culpable. If a school laptop is used at home for personal use then it might be a taxable benefit.	Laptop
Make sure that personal data is stored in the correct place	The best place for the safe storage of personal data (educators or learners) is on the school network or a secure remote service such as the OneDrive. Only use memory sticks or CDs for the transfer of personal data and wipe them clean afterwards. The storage of personal data on a laptop is to be discouraged. If it is necessary then be careful that personal data on laptops is encrypted and password protected.	
Always lock your keyboard if you are not near the computer:	 Lock your Windows XP computer.	Passwords
Always have a secure password that you shield from student's view.	Use the letters from a phrase and include numbers and capital letters. **M**y **s**on **D**avid **i**s twenty two **y**ears **o**ld: MsDi22yo http://www.microsoft.com/protect/yourself/password/checker.mspx will check your password strength.	
Never use a personal email for school business	All educators in Somerset have an email account that can be accessed through Office 365. https://outlook.com/kingsmead-school.com or through https://portal.office.com This account is maintained by ICT Services and will have all the latest security procedures and settings.	E-mails
Treat all emails as public documents	Emails can easily by misdirected by you or forwarded by others. Be careful that what	

	you write is accurate and be careful that you send only to the correct people. Ask for the email address if you are not sure.	
Only use Social Networking Sites for educational purposes if they have been agreed by the Senior Management.	Staff need an online environment that is under their control. Users must be authenticated. A Local Authority provided or recommended communication and collaboration area will have a range of security features set within a policy framework. Logs should be available in case a false allegation is made.	Sc
Make sure that all privacy settings on Social networking sites are set correctly	 	
Only accept people you know as friends on Social Networking Sites **Never** accept students and be very careful about accepting ex-students as friends on Social Networking Sites		king and Gaming
Be careful about what you publish – even if security settings have been used.	Information once published is impossible to control and may be manipulated without your consent, used in different contexts or further distributed. Do not publish anything that you would not want your mum, children or boss to see, either now or in ten years' time! Treat any conversation as if it was in a shop queue. If it is not appropriate then you could be accused of professional misconduct.	
Always report 'malicious' remarks, comments etc	If you find any information that you are not sure about then report it immediately to your line manager or Management Team.	
If you are taking part in 'open' sites such as networked games then always use a pseudonym and never supply any details that could be used to identify you.	As with advice that we give to learners then never supply personal data or information that could be used to identify who you are.	

Never take photos using your mobile phone. Use the school's digital camera.	With a personal camera it would be more difficult for to prove that the pictures were not taken for inappropriate use. Memory cards should only provide a temporary storage for pictures – with them being uploaded to an appropriate area on the school's network as soon as possible.	Mobile Phone
Never give your mobile phone number to learners or carers	If the use of a mobile phone is important to an activity then the school should provide this resource.	
Make sure that the searches you are encouraging learners to use are carefully considered and are age related.	Direct user to particular sites or use safe search engines e.g. CBBC Safe with younger learners. With older learners you need to teach them how to search safely.	Safe Sites
Never check suspicious sites or emails without **written** permission of the School Management	An educator might, with the best of intent, check sites that a user has visited and email images to alert a colleague. Should the images prove to be illegal then the educator **has** committed an offence.	

Sexting – Response process for professionals

This flowchart (adapted from '*Medway Local Authority Response for Professionals')* will help you to make a decision about the actions you need to take