SOUTHERNWAY FEDERATION

E-SAFETY POLICY

Changes

Version: 8

September 2008:	Policy implemented
September 2010:	Policy developed
October 2015:	Policy reviewed & approved by Learning & Standards Committee
Next Review due:	October 2016

If you have any questions regarding this policy, please contact the Acting Executive Headteacher.

The implementation of this e-safety policy will be monitored by the:	*SLT and FLT members, technical and teaching staff, governors*
Monitoring will take place at regular intervals:	*Nov 2015 & Feb 2016*
The Governing Body 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:	*Last FGB meeting of each academic year (Steve Mann)*
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:	*Nov 2015 & Feb 2016*
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*

Background/Rationale

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

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

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

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside of school. Some of the dangers they may face include:

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

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

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

The Federation must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, whilst 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 communication technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This e-safety policy has been developed by the Southernway Federation E-safety Committee:

- School E-Safety Coordinator
- Acting Executive Headteacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

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

- Staff meetings
- Governors meeting / sub-committee meeting
- School website and newsletters

The Federation will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of:
  - pupils (eg Ofsted “Tell-us” survey / CEOP “ThinkUknow” survey)
  - parents / carers
  - staff

Scope of the Policy

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 Federation ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school but is linked to membership of the schools.

The schools will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

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 Learning & Standards Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the Learning & Standards Committee

Acting Executive Headteacher and Senior Leaders

- The Acting Executive Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Acting Executive Headteacher / Senior Leaders are 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 Acting Executive Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Acting Headteacher and another member of the Senior Leadership Team / 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. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures).

E-Safety Coordinator

- Leads the e-safety committee.
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.

- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the e-safety governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant Governor committee meetings.
- Reports regularly to Senior Leadership Team

Network Manager/Technical staff

The ICT Technician and ICT Co-ordinator are responsible for ensuring:

- That the Federation's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the Federation 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 schools' 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.
- The Federation's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single individual.
- 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 Acting Executive Headteacher / Senior Leader /ICT Co-ordinator / Class teacher (as in the section above) for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in Federation policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- they report any suspected misuse or problem to the Acting Executive Headteacher / Senior Leader / ICT Co-ordinator / Class teacher (as in the section above) 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.
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for Child Protection

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.

E-Safety Committee

Members of the E-Safety committee will assist the ICT c-oordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school (SWGfL) filtering policy.

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil 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 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 Federation's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The schools will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

- accessing the schools' website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Communiuty Users

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

Policy Statements

Education – Pupils

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

- A planned e-safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are included in the Acceptable Usage Policy, signed by all users.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – Parents/Carers

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

- Letters, newsletters, web site.
- Parents evenings.
- Reference to the SWGfL Safe website (NB the SWGfL "Golden Rules" for parents).

Education – Extended Schools

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

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the appraisal process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety and Acceptable Use Policies.
- The ICT Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The ICT Coordinator will provide advice / guidance / training as required to individuals as required.

Training – Governors

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

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

Technical – infrastructure/equipment, filtering and monitoring

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

- School ICT systems will be managed in ways that ensure that the Federation 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. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All users at KS2 and above will be provided with a username and password by technical support staff, who will keep an up to date record of users and their usernames. Users will be required to change their password every 2 terms

- The “administrator” passwords for the schools’ ICT system, used by the ICT co-ordinator / ICT Technician must also be available to the Acting Executive Headteacher or other nominated senior leader 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.
- The Federation maintains and supports the managed filtering service provided by SWGfL.
- In the event of the ICT Technician (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 Acting Executive Headteacher (or other nominated senior leader).
- 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 ICT co-ordinator and the E-Safety Committee. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- Federation 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.

  Remote management tools are used by staff to control workstations and view users’ activity.
- An appropriate system is in place of verbal and written communication for users to report any actual / potential e-safety incident to the ICT technician or the ICT co-ordinator.
- 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 development for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place whereby only administrators have permissions regarding the downloading of executable files by users.
- An agreed policy is being developed regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.

  An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place 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.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of computing 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, 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, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT co-ordinator or ICT technician can temporarily remove

those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The schools will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow Federation policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the schools' website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection - See Appendix 1

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

When using communication technologies the Federation considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person (SLT, SM, GW or PH) in accordance with Federation policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, 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.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use. (These remain contained within our network.)
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the schools' website and **only school office email addresses** should be used.

Unsuitable / inappropriate activities

The Federation 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 Federation policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for	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 (educational)		*				
On-line gaming (non educational)			*			
On-line gambling					*	
On-line shopping / commerce				*		
File sharing					*	
Use of social networking sites					*	
Use of video broadcasting eg Youtube				*		

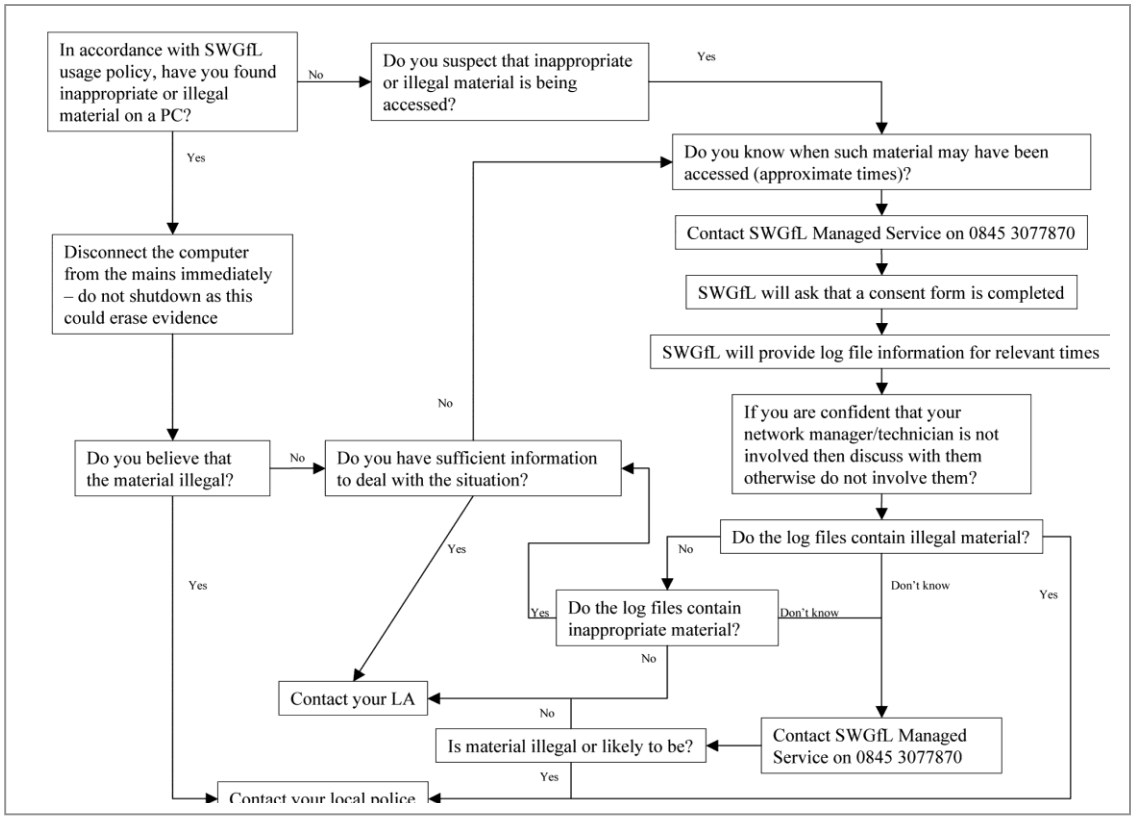
Responding to incidents of misuse

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 SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher	Refer to FLT / SLT / SM/GW/PH	Refer to Acting Executive Headteacher	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			*			*		*	*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			*			*	*	*	*
Using proxy sites or other means to subvert the school's filtering system			*			*	*		
Accidentally accessing offensive or pornographic material and failing to report the incident		*	*			*			
Deliberately accessing or trying to access offensive or pornographic material			*	*		*	*	*	*
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		*	*					*	*

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Acting Exec Head	RRefer 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	*	*				*		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	*	*				*		*
Careless use of personal data eg holding or transferring data in an insecure manner		*				*		*
Deliberate actions to breach data protection or network security rules		*	*					*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		*	*	*			*	*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		*	*			*		*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	*	*	*			*		
Actions which could compromise the staff member's professional standing		*				*		*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		*				*		*
Using proxy sites or other means to subvert the school's filtering system		*	*		*	*		*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*			*	*		
Deliberately accessing or trying to access offensive or pornographic material		*	*	*			*	*
Breaching copyright or licensing regulations	*					*		
Continued infringements of the above, following previous warnings or sanctions	*	*	*	*	*	*	*	*

Pupil Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The Federation will try to ensure that *pupils* will have good access to ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- **I will not communicate with others online** unless I have been instructed to (and supervised) by an adult.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing
- I will not use the school ICT systems for video/photo broadcasting (e.g. YouTube/blogging), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- **I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.**
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Policy (AUP), to which it is attached and visible on the Schools' website.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school).
- I use my own equipment in school (when allowed) e.g. mobile phones, laptops, PCs, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. **communicating with other members of the school**, accessing school email, online storage, website etc.

Name of Pupil	
Class	

Signed		Date	

Staff (and Volunteer) Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The Federation will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use Federation ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, social media, etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- **I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.**
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Federation's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are

published (e.g. on the schools' website / blog) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Federation and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schools:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the Federation about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant Federation policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Federation Personal Data Policy. Where personal data is transferred outside the secure school network, **it must be encrypted**.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Federation policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the Federation.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Federation ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Parent / Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The Federation will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I understand that if I need to contact school staff that I will do this via the appropriate channels, i.e. phone call, letter or an email sent to the school office. I **will not** contact members of school staff using their direct school email.

I understand that if my son/daughter does not follow the acceptable usage policy that ICT access may be withdrawn.

Signed		Date	

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names, unless permission has been sought from their parent/carer.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

I agree that I will not share any images on any social networking sites in accordance with the Federation Photographic Policy.

Signed		Date	

Data Protection Policy

E-Safety Policy - Appendix 1

Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive.

It is the responsibility of **all members** of the school community to take care when handling, using or transferring personal data that it can not be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements

The Federation will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The Federation and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities
The Federation's Senior Risk Information Officer (SIRO) is **Jackie Sparrow**, the Acting Executive Headteacher. She will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The Federation will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

Everyone in the Federation has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration
The Federation schools are each registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers /School Workforce – the "Privacy Notice"
Under the "Fair Processing" requirements in the Data Protection Act, the schools will inform parents / carers of all pupils / students and all members of the school workforce of the data they hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, NCA, etc) to whom it may be passed. This Privacy Notice will be passed to parents / carers/ school workforce through written notification if requested or direction to the Policy area of the Website. Parents / carers of young people/ members of the school workforce who are new to the schools will be provided with the Privacy Notice through either of the above methods.

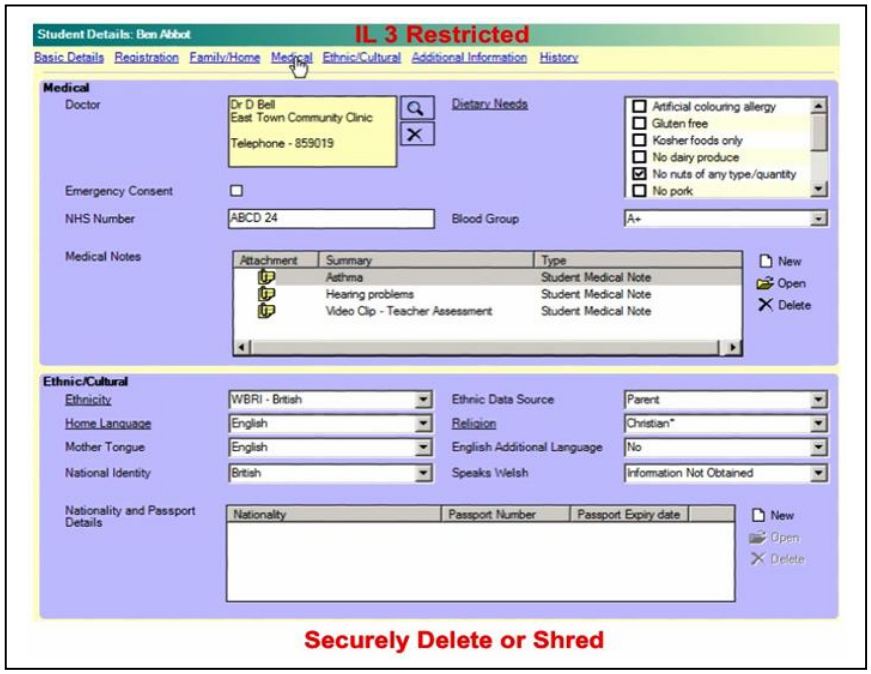
Training & awareness
All staff will receive data handling awareness training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Identification of data

The Federation will ensure that all school staff, contractors working for it, and delivery partners comply with restrictions applying to the access to, handling and storage of data classified as ***Protected, Restricted*** or higher.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer:



Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect
- IL3–Restricted
- IL4–Confidential

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data.

Release and destruction markings will be shown in the footer as follows:

[Release],		**[Parties],**		**[Restrictions].**		**[Encrypt, Securely delete or shred]**
The authority descriptor		The individuals or organisations the information may be released to		Descriptor tailored to the specific individual		How the document should be destroyed
Examples:						
Senior Information Risk Owner		School use only		No internet access No photos		Securely delete or shred
Teacher		Mother only		No information to father ASBO		Securely delete or shred

Secure storage of and access to data
The Federation will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and choose strong passwords which must be changed regularly – once per term. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

When personal data is stored on any portable computer system, USB stick or any other removable media, the data must be encrypted. All members of the organisation are advised not to store data locally or remove it from the network/premises. If individuals choose to ignore this advice the responsibility for encrypting the data lies with the individual.

The Federation has clear policy and procedures for the backing up of all data held on the school systems, including multiple network back-ups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The Federation recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests, i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school
The Federation recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software (truecrypt/axcrypt).
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. **(Please note: in some countries, carrying encrypted data is ILLEGAL).**

Disposal of data
The Federation will comply with the requirements for the safe destruction of sensitive data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging / Reporting / Incident Handling
As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals- Jackie Sparrow (Acting Executive Headteacher), Steve Mann (ICT coordinator) or Paul Howlett (ICT Technician).
The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.
The Federation has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and

- a plan of action of non-recurrence and further awareness raising.

Any loss or suspected breach of this policy should be immediately reported to either the relevant IAO or SIRO.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further reading
Cabinet Office – Data handing procedures in Government – a final report
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

Notice to parents:

PRIVACY NOTICE

Pupils in Schools, Academies, Alternative Provision, Pupil Referral Units and children in Early Years Settings

Privacy Notice - Data Protection Act 1998

We **Beechwood & Oakwood Primary Schools** are the data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information [1] and personal characteristics such as your ethnic group, special educational needs and any relevant medical information. *If you are enrolling for post 14 qualifications we will be provided with your unique learner number by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.*

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some of your information to the Local Authority and the Department for Education (DfE).
If you want to see a copy of the information we hold and share about you then please contact **your School Office.**

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

Local Authority:
http://www.plymouth.gov.uk/homepage/education/schools/schoolprivacynotice.htm
http://www.plymouth.gov.uk/homepage/staffroom/schoolroom/usefuldocuments/modelpolicies.htm
DfE: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites, please contact the LA or DfE as follows:

[1] Attendance information is **NOT** collected as part of the Censuses for the Department for Education for the following pupils / children - a) in Nursery schools; b) aged under 4 years in Maintained schools; c) in Alternative Provision; and d) in Early Years Settings.

DfE
Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: https://www.gov.uk/government/organisations/department-for-education
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

LA
Policy, Performance and Partnerships Team
Floor 3, Ballard House, West Hoe Road
Plymouth City Council
Plymouth
Devon
PL1 3BJ
Website: www.plymouth.gov.uk
Email: PPP@plymouth.gov.uk
Tel: 01752 398330

Notice to School Workforce:

PRIVACY NOTICE

School Workforce: those employed or otherwise engaged to work at a school or the Local Authority

Privacy Notice - Data Protection Act 1998

We **the Southernway Federation** are the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the Federation about those employed or otherwise engaged to work at the school or Local Authority. This is to assist in the smooth running of the Federation and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body and the School Support Staff Negotiating Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:

- the Plymouth City Council
- the Department for Education (DfE)

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- http://www.plymouth.gov.uk
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites, please contact the Plymouth City Council or DfE as follows:

Plymouth City Council
Policy, Performance and Partnerships Team
Floor 3, Ballard House, West Hoe Road
Plymouth City Council
Plymouth
Devon
PL1 3BJ

Website: http://www.plymouth.gov.uk/homepage/education/schools/schoolprivacynotice.htm

Email: PPP@plymouth.gov.uk

Tel: 01752 398330

DfE
Public Communications Unit
Department for Education, Sanctuary Buildings
Great Smith Street, London
SW1P 3BT

Website: https://www.gov.uk/government/organisations/department-for-education

Email: info@education.gsi.gov.uk

Telephone: 0370 000 2288.

E-Safety Policy 2015 / 2016

Appendix 2 – Password Security Policy

Introduction

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

- users can only access data to which they have right of access
- no user should be able to access another's files without permission
- access to personal data is securely controlled in line with the Federation's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Google Apps.

Responsibilities

The management of the password security policy will be the responsibility of Jackie Sparrow (Acting Executive Headteacher), Steve Mann and Paul Howlett.

All users (adults and young people) 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.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT Technician with a prompt to change it at the first logon. Any changes carried out must be notified to the manager of the password security policy (above).

Users will change their passwords every new term.

Passwords must not be simple words or combinations of words contained within the dictionary (any language).
Each password must contain upper and lower case letters, numbers/ symbols.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in ICT and / or e-safety lessons
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).

All users at KS2 will be provided with a username and password by the ICT coordinator who will keep an up to date record of users and their usernames. Users will be required to change their password every two terms.

Users at KS1 and below will use group logons.

The following rules apply to the use of passwords:

- passwords must be changed every new term (staff) / two terms (KS2)
- the last four passwords cannot be re-used
- the password should be a minimum of 6 characters long and
- must include three of – uppercase character, lowercase character, number, special character
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

The "administrator" passwords for the Federation ICT system, used by the Network Manager (or other person) must also be available to the Acting Executive Headteacher or other nominated senior leader and kept in a secure place (eg school safe).

Audit / Monitoring / Reporting / Review

The responsible person (Jackie Sparrow Acting Executive Headteacher/Steve Mann/ Paul Howlett) will ensure that full records are kept of:

- User IDs, passwords and password changes
- User log-ons
- Security incidents related to this policy

These records will be reviewed by the E-Safety Officer at regular intervals.

This policy will be regularly reviewed (annually) in response to changes in guidance and evidence gained from the logs.

Southernway Federation Oakwood/Beechwood Primary

2015/16 Staff AUP Agreement Register

I have read and understand the e-document (2015/16 Staff AUP) and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	Signature	Date

Name	Signature	Date
Name	Signature	Date

Name	Signature	Date
Name	Signature	Date

Name	Signature	Date
Name	Signature	Date