



**STATUS: APPROVED**

**APPROVED BY: GOVERNING BODY**

**DATE:**

## **NORTHAM SCHOOLS FEDERATION E-SAFETY POLICY**

### Introduction

Northam Federations Federation E-Safety Policy has been written by the federation, building on the South West Grid for Learning (SWGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

This Policy document is drawn up to protect all parties – the students, the staff and the federation and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Northam Federations Federation recognises that new technologies have become integral to the lives of children and young people in today's society, both within federations and in their lives outside federation.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children 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 use of these exciting and innovative tools in federation and at home has been shown to raise educational standards and promote children's achievement. However, the use of these new technologies can put young people at risk within and outside the federation. 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.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children's 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.

This policy applies to all members of the federation community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of federation ICT systems, both in and out of the federation.

The Education and Inspections Act 2006 empowers Executive Headteachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the federation 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 federation, but is linked to membership of the federation.

The federation 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 federation.

### **Roles and Responsibilities**

The following section outlines the roles and responsibilities for e-safety within the federation:

#### **Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor

#### **Executive Headteacher and Senior Leaders:**

- The Executive Headteacher is responsible for ensuring the safety (including e-safety) of members of the federation community.
- The Executive Headteacher will ensure that there is a system in place to allow for monitoring and support of those in federation who carry out the internal e-safety monitoring role.
- The Executive Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

#### **E-Safety Coordinator:**

- has a leading role in establishing and reviewing the federation e-safety policies / documents
- provides training and advice for staff
- liaises with the Local Authority
- liaises with federation ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

#### **ICT Technician**

The ICT Technician is 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 federation's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role.
- they monitor ICT activity in lessons

#### **Teaching and Support Staff:**

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current federation e-safety policy and practices
- they have read, understood and signed the federation Staff Acceptable Use Policy / Agreement (AUP)

- they report any suspected misuse or problem to the E-Safety Co-ordinator /Executive Headteacher
  - digital communications with pupils should be on a professional level
  - e-safety issues are embedded in all aspects of the curriculum and other federation 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 federation 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
- Child Protection Coordinator is 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

#### **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 federation will therefore take every opportunity to help parents understand these issues.

#### **Community Users:**

Community Users who access federation ICT systems as part of the Extended Federation provision will be expected to sign a Community User AUP before being provided with access to federation systems.

Safe use of ICT systems within Federation – The following section defines expectations for safe use of ICT Equipment

Federation ICT suite, Network and Laptops - Technical – infrastructure / equipment, filtering and monitoring

The federation will be responsible for ensuring that the federation infrastructure / network is as safe and secure as is

reasonably possible and that policies and procedures approved within this policy are implemented.

- Federation 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 federation ICT systems

- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to federation ICT systems. 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.

- All staff will be provided with a username and password 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 administrator passwords for the federation ICT system, used by the Network Manager (or other person) must also be available to the Executive Headteacher or other nominated senior leader and kept in a secure place

The federation maintains and supports the managed filtering service provided by SWGfL

- 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 federation systems and data.

# Policy Statements

## Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in e-safety is therefore an essential part of the federation's e-safety provision. Children and young people need the help and support of the federation to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways: *(statements will need to be adapted, depending on the age of the students / pupils and the federation's structure)*

- **A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in federation and outside federation**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / 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**
- *Students / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside federation*
- *Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet*
- *Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens*
- *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: *(select / delete as appropriate)*

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

## Education - Extended Federations

*The federation will offer family learning courses in ICT, media literacy 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: *(select / delete as appropriate)*

- **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 performance management process.*
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the federation e-safety policy and Acceptable Use Policies**
- *The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator (or other nominated person) 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 ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

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

## Technical – infrastructure / equipment, filtering and monitoring

*(nb. if the federation has a managed ICT service provided by an outside contractor, it is the responsibility of the federation to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the federation, as suggested below. It is also important that the managed service provider is fully aware of the SWGfL Security Policy and Acceptable Usage Policy.)*

*(nb the federation should also check their Local Authority policies on these technical issues)*

**The federation will be responsible for ensuring that the federation 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:** *(federations will have very different ICT infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:)*

- **Federation 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 federation ICT systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to federation 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 and above) will be provided with a username and password** *by (insert name or title) who will keep an up to date record of users and their usernames. Users will be required to change their password every (insert period). (Federations may choose to use group or class log-ons and passwords for KS1 and below, but need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access. Federations should also consider the implications of the development of Learning Platforms and home*

access on whole class log-ons and passwords. A federation password policy template is provided in the appendix to this document)

- **The “master / administrator” passwords for the federation ICT system, used by the Network Manager (or other person) must also be available to the Executive Headteacher or other nominated senior leader and kept in a secure place (eg federation safe)**

(Alternatively, where the system allows more than one “master / administrator” log-on, the Executive Headteacher or other nominated senior leader should be allocated those master / administrator rights. A federation should never allow one user to have sole administrator access)

- *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 (nb. in the unusual event that the federation has decided to remove the SWGfL filtering and replace it with another filtering system, this should be clearly explained in the policy and evidence provided that the Executive Headteacher would be able to show, in the event of any legal issue that the federation was able to meet its statutory requirements to ensure the safety of staff / students / pupils)*
- *(possible statement) The federation has provided enhanced user-level filtering through the use of the (insert name) filtering programme.*
- *In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the 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 Network Manager and (insert name or title) (nb an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). 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 federation ICT systems and users are made aware of this in the Acceptable Use Policy. (federations may wish to add details of the monitoring programmes that are used).*
- *(possible statement) Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).*
- *Appropriate security measures are in place (federations may wish to provide more detail) 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 federation systems and data.*
- *An agreed policy is in place (to be described) for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the federation system.  
An agreed policy is in place (to be described) regarding the downloading of executable files by users*
- *An agreed policy is in place (to be described) 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 federation. (see Federation Personal Data Policy Template in the appendix for further detail)*
- *An agreed policy is in place (to be described) that allows staff to / forbids staff from installing programmes on federation workstations / portable devices.*
- *An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on federation workstations / portable devices. (see Federation Personal Data Policy Template in the appendix for further detail)*
- *The federation infrastructure and individual workstations are protected by up to date virus software.*
- *Personal data can not be sent over the internet or taken off the federation site unless safely encrypted or otherwise secured. (see Federation Personal Data Policy Template in the appendix for further detail)*

# Curriculum

**E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.**

- *in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) 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.*
- *Students / 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*
- *Students / 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 students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / 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 federation will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: *(select / delete as appropriate)*

- **When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- *Staff are allowed to take digital / video images to support educational aims, but must follow federation policies concerning the sharing, distribution and publication of those images. Those images should only be taken on federation equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the federation into disrepute.*
- *Students / pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Students' / 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 students / pupils are published on the federation website (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix)*
- *Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

## 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:



Taking photos on mobile phones or other camera devices								
Use of hand held devices eg PDAs, PSPs								
Use of personal email addresses in federation, or on federation network								
Use of federation email for personal emails								
Use of chat rooms / facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								

The federation may also wish to add some policy statements about the use of communications technologies, in place of, or in addition to the above table:

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

- **The official federation email service may be regarded as safe and secure and is monitored.** *Staff and students / pupils should therefore use only the federation email service to communicate with others when in federation, or on federation systems (eg by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the 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 students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) federation 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 students / pupils at KS2 and above will be provided with individual federation email addresses for educational use. (Federations may choose to use group or class email addresses for younger age groups eg. at KS1)*
- *Students / 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 federation website and only official email addresses should be used to identify members of staff.*

## Unsuitable / inappropriate activities

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

The federation believes that the activities referred to in the following section would be inappropriate in a federation context and that users, as defined below, should not engage in these activities in federation or outside federation when using federation equipment or systems. The federation policy restricts certain internet usage as follows:

(the federation should agree its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues)

(The last section of the table has been left blank for federations to decide their own responses)

## User Actions

		Acceptable	Acceptable at	Acceptable for	Unacceptable	Unacceptable
<b>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:</b>	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 federation or brings the federation into disrepute				?		
Using federation 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 federation					?	
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						

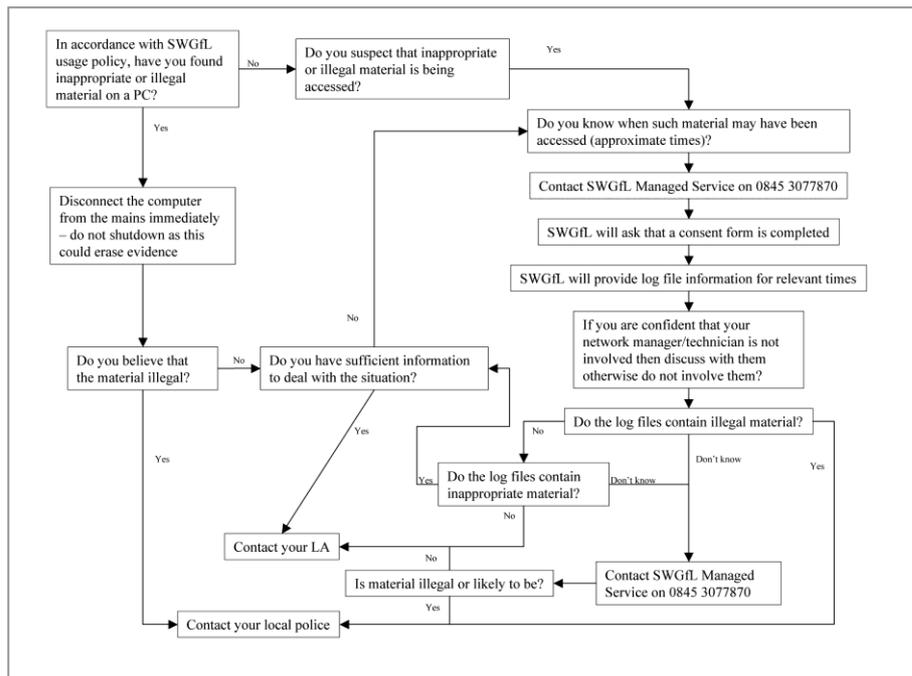
## Responding to incidents of misuse

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

**If any apparent or actual misuse appears to involve illegal activity ie.**

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

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



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 federation 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: (the federation will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues)

**Students / Pupils**

**Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to 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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		?	?	?					
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 federation network by sharing username and passwords									
Attempting to access or accessing the federation network, using another student's / pupil's account									
Attempting to access or accessing the federation 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 federation into disrepute or breach the integrity of the ethos of the federation									
Using proxy sites or other means to subvert the federation's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Executive Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		?	?	?				
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 federation network by sharing username and passwords or attempting to access or accessing the federation 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 federation into disrepute or breach the integrity of the ethos of the federation								
Using proxy sites or other means to subvert the federation'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								

# Appendices

Can be found on the following pages:

• Student / Pupil Acceptable Usage Policy template	25
• Staff and Volunteers Acceptable Usage Policy template	28
• Parents / Carers Acceptable Usage Policy Agreement template	31
• Federation Filtering Policy template	33
• Federation Password Security Policy template	36
• Federation Personal Data Policy template	39
• Federation E-Safety Charter	46
• Ideas for federations to consider	47
• Legislation	49
• Links to other organisations and documents	52
• Resources	54
• Glossary of terms	55

# Student / Pupil Acceptable Use Policy Agreement Template

Sections that include advice or guidance are written in RED. It is anticipated that federations will remove these sections from their final AUP document. Federations should review and amend the contents of this AUP to ensure that it is consistent with their E-Safety Policy and other relevant federation policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AUP Agreement will be more concise.

## Federation Policy

New technologies have become integral to the lives of children and young people in today's society, both within federations and in their lives outside federation. 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 federation 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 *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* 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.

For my own personal safety:

- I understand that the federation 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.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- 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 federation 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 federation ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.  
(federations should amend this section to take account of their policy on each of these issues)

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 federation has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the federation:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in federation if I have permission (federations should amend this section in the light of their mobile phone / hand held devices policies). I understand that, if I do use my own devices in federation, I will follow the rules set out in this agreement, in the same way as if I was using federation 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.
- I will only use chat and social networking sites with permission and at the times that are allowed (federations should amend this section to take account of their policy on access to social networking and similar sites)

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 federation:

- I understand that the federation 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 federation and where they involve my membership of the federation 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 (federations should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the federation network / internet, detentions, suspensions, 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 federation ICT systems.**

## Student / Pupil Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Policy (AUP), to which it is attached.

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 federation ICT systems.

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

- I use the federation ICT systems and equipment (both in and out of federation)
- I use my own equipment in federation (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of federation in a way that is related to me being a member of this federation eg communicating with other members of the federation, accessing federation email, VLE, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

# Staff (and Volunteer) Acceptable Use Policy Agreement Template

Sections that include advice or guidance are written in RED. It is anticipated that federations will remove these sections from their final AUP document. Federations should review and amend the contents of this AUP to ensure that it is consistent with their E-Safety Policy and other relevant federation policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AUP will be more concise.

## Federation Policy

New technologies have become integral to the lives of children and young people in today's society, both within federations and in their lives outside federation. 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. 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 federation 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 *students / 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 students / 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 federation 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 federation ICT systems (eg laptops, email, VLE etc) out of federation. (federations should amend this section in the light of their policies which relate to the use of federation systems and equipment out of federation)
- I understand that the federation 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 federation. (federations should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of federation systems)
- 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 federation ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- 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 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 (eg on the federation website / VLE) 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 federation in accordance with the federation's policies. (federations should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official federation systems. Any such communication will be professional in tone and manner. (federations should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- 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 federation:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in federation, I will follow the rules set out in this agreement, in the same way as if I was using federation 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. (federations should amend this section in the light of their policies which relate to the use of staff devices)
- I will not use personal email addresses on the federation ICT systems. (federations should amend this section in the light of their email policy – some federations will choose to allow the use of staff personal email addresses in federation)
- 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 federation policies. (federations should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to federation 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 / LA Personal Data Policy (or other relevant federation policy). Where personal data is transferred outside the secure federation network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / 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 federation 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 federation:

- I understand that this Acceptable Use Policy applies not only to my work and use of federation ICT equipment in federation, but also applies to my use of federation ICT systems and equipment out of federation and my use of personal equipment in federation 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 (federations should amend this section to provide relevant sanctions as per their behaviour policies) 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 federation) and my own devices (in federation and when carrying out communications related to the federation) within these guidelines.

Staff / Volunteer Name

Signed

Date

## Parent / Carer Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within federations and in their lives outside federation. 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 federation 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 *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the federation expectations of the young people in their care.

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

### Permission Form

Parent / Carers Name

Student / Pupil Name

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

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 federation.

I understand that the federation 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 federation 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 federation 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 federation if I have concerns over my child's e-safety.

Signed

Date

## Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of federation. 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 federation website and occasionally in the public media,

The federation will comply with the Data Protection Act and request parents / carers permission before taking images of members of the federation. We will also ensure that when images are published that the young people can not be identified by the use of their names. Parents are requested to sign the permission form below to allow the federation to take and use images of their children.

### Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the federation 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 federation.

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

Signed

Date

### Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

It is suggested that when the Student / Pupil AUP is written that a copy should be attached to the Parents / Carers AUP Agreement to provide information for parents and carers about the rules and behaviours that students / pupils have committed to by signing the form.

# Federation Filtering Policy Template

SWGfL federations automatically receive a filtered broadband service. Details of the SWGfL Internet Filtering Service and Policy can be found at:

<http://www.swgfl.org.uk/safety/default.asp>. This service is intended to prevent users accessing material that would be regarded as illegal and / or inappropriate in an educational environment, as defined in the Filtering Policy. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

The SWGfL filtering service provides flexibility for federations to decide on their own levels of filtering security. It is possible to add to or override some of the sites filtered by SWGfL.

As the use of the internet becomes more widespread, access becomes available through a wider range of technologies and users become more sophisticated in their internet use, federations need to continually review their filtering and monitoring policies.

Many users are not aware of the flexibility available at a local level for federations, and other organisations, connected to SWGfL and its filtering service. Federations should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

The template document below provides a basis for a federation filtering policy. Federations will however need to consider carefully the issues raised and decide:

- Whether they will adopt the SWGfL Filtering Policy without change
- Whether to allow flexibility for sites to be added or removed from the filtering list for your organisation.
- Whether to remove filtering controls for some internet use (eg social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used.

In the template below, sections of guidance will be written in RED, while sections shown in bold indicate those elements of the policy that are strongly recommended by SWGfL. Sections in italics indicate those elements that the federation will need to consider and decide whether to include or not.

## Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the federation has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this federation.

As a part of the South West Grid for Learning (SWGfL) federations and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

## Responsibilities

The responsibility for the management of the federation's filtering policy will be held by (insert title – federations may choose to consider – Network Manager / ICT Technician / Head of ICT etc). They will manage the federation filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL / federation filtering service must (federations should choose their relevant response(s):

- **be logged in change control logs**
- **be reported to a second responsible person (insert title):**

- *either... be reported to and authorised by a second responsible person prior to changes being made (recommended)*
- *or... be reported to a second responsible person (insert title) every X weeks / months in the form of an audit of the change control logs*
- *be reported to the E-Safety Governor every X weeks / months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the federation's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

### Education / Training / Awareness

*Pupils / students* will be made aware of the importance of filtering systems through the e-safety education programme (*federations may wish to add details*). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (*amend as relevant*)

- *signing the AUP*
- *induction training*
- *staff meetings, briefings, Inset.*

Parents will be informed of the federation's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc. (*amend as relevant*)

### Changes to the Filtering System

In this section the federation should provide a detailed explanation of:

- *how, and to whom, users may request changes to the filtering*
- *the grounds on which they may be allowed or denied (federations may choose to allow access to some sites eg social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).*
- *how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)*
- *any audit / reporting system*

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make federation level changes (as above). If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the responsible person (insert title) should email [filtering@swgfl.org.uk](mailto:filtering@swgfl.org.uk) with the URL.

## Monitoring

Some federations supplement their filtering systems with additional monitoring systems. If this is the case, federations should include information in this section, including – if they wish – details of internal or commercial systems that are in use.

*No filtering system can guarantee 100% protection against access to unsuitable sites. The federation will therefore monitor the activities of users on the federation network and on federation equipment as indicated in the Federation E-Safety Policy and the Acceptable Use agreement. Monitoring will take place as follows: (details should be inserted if the federation so wishes).*

## Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (federations should amend as relevant)

- *the second responsible person (insert title)*
- *E-Safety Committee*
- *E-Safety Governor / Governors committee*
- *SWGfL / Local Authority on request*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case federations might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

# Federation Password Security Policy Template

## Introduction

The federation will be responsible for ensuring that the *federation 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 (or as allowed for monitoring purposes within the federation's policies).
- 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 federation ICT systems, including email and Virtual Learning Environment (VLE).

## Responsibilities

The management of the password security policy will be the responsibility of *(insert title)* (federations will probably choose the Network Manager / ICT Technician / Head of ICT or other relevant responsible person)

All users (adults and young people) will have responsibility 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. (If the federation decides to provide "class log-ons" at Key Stage 1, they will need to amend the wording of this section)

*Passwords for new users, and replacement passwords for existing users can be allocated by xxxxx (insert title) (federations may wish to have someone other than the federation's technical staff carrying out this role eg an administrator who is easily accessible to users). Any changes carried out must be notified to the manager of the password security policy (above).*

*Users will change their passwords every xxxx (to be decided by the federation – it is recommended that this should be at least every 90 days, some organisations require changes each month)*

## Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

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

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

Pupils / students will be made aware of the federation's password policy:

- in ICT and / or e-safety lessons (the federation should describe how this will take place)
- through the Acceptable Use Agreement

## Policy Statements

All users will have clearly defined access rights to federation 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 and above) will be provided with a username and password by (insert name or title) who will keep an up to date record of users and their usernames. Users will be required to change their password every (insert period). (Federations may choose to use group or class log-ons and passwords for KS1 and below, but need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access. Federations should also consider the implications of the development of Learning Platforms and home access on whole class log-ons and passwords)

The following rules apply to the use of passwords: (federations will need to take account of local authority guidance and the level of security required factored against the ease of access required for users)

- *passwords must be changed every xxxx*
- *the last four passwords cannot be re-used*
- *the password should be a minimum of 8 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)*
- *requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the federation will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)*

Where sensitive data is in use – particularly when accessed on laptops – federations may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

The “master / administrator” passwords for the federation ICT system, used by the Network Manager (or other person) must also be available to the Executive Headteacher or other nominated senior leader and kept in a secure place (eg federation safe). (Alternatively, where the system allows more than one “master / administrator” log-on, the Executive Headteacher or other nominated senior leader should be allocated those master / administrator rights. A federation should never allow one user to have sole administrator access).

## Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by ... (*E-Safety Officer / E-Safety Committee / E-Safety Governor*) at regular intervals (*state the frequency*).

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

# Federation Personal Data Handling Policy Template

Recent publicity about the loss of personal data by organisations and individuals has made this a current and high profile issue for federations and other organisations. It is important that the federation has a clear and well understood personal data policy because:

- No federation or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Federations are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The federation will want to avoid the criticism and negative publicity that could be generated by any loss of personal data.
- The federation is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Federations have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in federation but also from remote locations. Legislation covering the safe handling of this data is addressed by the UK Data Protection Act 1998 and following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in federations, it is critical that they adopt these procedures too.

It is important to stress that the Personal Data Policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. As it is part of an overall e-safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

**Federations will need to carefully review this policy template and amend sections, as necessary, in the light of pertinent Local Authority regulations and guidance, and changes in legislation.**

## Introduction

Federations should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becta – Good Practice in information handling in federations – keeping data secure, safe and legal – Sept 2008).

It is the responsibility of all members of the federation 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 federation into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

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. (federations will need to check on this)

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. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the federation community – including *pupils / students*, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg 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 (*insert name or title*). (**Federations may choose to combine this role with that of Data Protection Officer**). They will keep up to date with current legislation and guidance and will:

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

The federation will identify Information Asset Owners (IAOs) (**the federation may wish to identify these staff by name or title in this section**) for the various types of data being held (eg pupil / student 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

**Federations are recommended to adopt the SIRO and IAO positions in the Becta document – “Good Practice in information handling in federations ... ” – see further reading section at the end of this template document.**

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 is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. (**federations are responsible for their own registration**)

## Information to Parents / Carers – the “Fair Processing Notice”

Under the “Fair Processing” requirements in the Data Protection Act, the federation will inform parents / carers of all pupils / students of the data they hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, Connexions etc) to whom it may be passed. This fair processing notice will be passed to parents / carers through ... (to be inserted – federations might choose to use the Prospectus, newsletters, reports or a specific letter / communication). Parents / carers of young people who are new to the federation will be provided with the fair processing notice through. (to be inserted – as above)

A copy of a specimen fair processing notice can be found at:

<http://www.teachernet.gov.uk/management/ims/datamanagement/fnpupils/>. It contains a relevant wording for the regulations pertaining to the transfer of information to Connexions, in secondary federations and new requirements resulting from the introduction of ContactPoint. A new specimen FPN is available for 2008/9. Federations are advised to contact their Local Authority for local versions of the Fair Processing Notice.

## Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through: (federations should amend or add to as necessary)

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners (or insert titles of relevant persons)

## Identification of data

The federation will ensure that all federation staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, 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:

The screenshot shows a web interface for a student profile. At the top, it says "IL 3 Restricted". Below this are several tabs: "Basic Details", "Registration", "Family Home", "Medical", "Ethnic/Cultural", "Personal Information", and "History". The "Medical" tab is selected. The "Medical" section includes fields for "Doctor" (Dr D Bell, East Town Community Clinic, Telephone: 059015), "Emergency Consent" (checkbox), "NHS Number" (BCC 24), and "Blood Group" (A-). There is a "Dietary Needs" section with checkboxes for "Artificial colouring/ally", "Gluten free", "Kosher foods only", "No dairy produce", "No nuts of any type - quantity", and "No pork". Below this is a "Medical Notes" table with columns for "Attachment", "Summary", and "Type". The table contains three rows: "Asthma" (Student Medical Note), "hearing problems" (Student Medical Note), and "Video Clip - Teacher Assessment" (Student Medical Note). There are "New", "Open", and "Delete" buttons for the notes. The "Ethnic/Cultural" section includes dropdown menus for "Ethnicity" (WBI - British), "Ethnic Data Source" (Parent), "Home Language" (English), "Religion" (Christian), "Mother Tongue" (English), "English Additional Language" (No), "National Identity" (British), and "Speaks Welsh" (Information Not Obtained). At the bottom, there is a "Nationality and Passport Details" section with fields for "Nationality", "Passport Number", and "Passport Expiry date", and "New", "Open", and "Delete" buttons. At the very bottom of the page, it says "Securely Delete or Shred".

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: (the table below is taken from Becta guidance. Federations will need to decide, in line with LA Guidance how their data is marked)

[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
<b>Examples:</b>			
Senior Information Risk Owner	Federation use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information to father ASBO	Securely delete or shred

Becta guidance recommends that educational ICT systems should be set up to label the output of any protected data as being IL3-Restricted by default and that federations should consider this when procuring new ICT systems.

Becta is working with suppliers to investigate solutions for the incorporation of implicit labelling within MIS and learning platforms. Where systems are inter-connected, appropriate security must be provided in the end system (that is, the system that aggregates the data), together with supporting procedural measures.

As of September 2008, the vast majority of systems do not enforce data protection on the basis of Impact Level labels.

Federations will need to review the above section with regard to LA policies, which may be more specific, particularly in the case of HR records.

### 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 strong passwords which must be changed regularly (insert relevant federation details as per the federation's password security policy). 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.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on federation equipment (this includes computers and portable storage media) (where allowed). Private equipment (ie owned by the users) must not be used.

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 (below) once it has been transferred or its use is complete

The federation will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.

The federation has clear policy and procedures for the automatic backing up, accessing and restoring all data held on federation systems, including off-site backups. (the federation will need to set its own policy, relevant to its physical layout, type of ICT systems etc)

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 (insert details here) to deal with Subject Access Requests ie. 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 federation

The federation recognises that personal data may be accessed by users out of federation, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the federation or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location. (see earlier section – LA / federation policies may forbid such transfer)
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of federation.
- When data is required by an authorised user from outside the federation 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.
- 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. (nb. to carry encrypted material is illegal in some countries)

(Federations will find detailed guidance on data encryption in the Becta document “Good practice in information handling in federations – Data Encryption - a guide for staff and contractors tasked with implementing a system of secure data encryption and deletion”)

### Disposal of data

The federation will comply with the requirements for the safe destruction of personal 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 (see further reading section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

*A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

### **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. (insert name or title)

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.

(Federations will find detailed guidance on audit logging in the Becta document “Good practice in information handling in federations - audit logging and incident handling - a guide for staff and contractors tasked with implementing data security”)

The federation has a policy for reporting, managing and recovering from information risk incidents, which establishes: (federations should determine their own reporting policy, in line with that of their LA, and add details here)

- 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.

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

Teachernet – Data processing and sharing -

<http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/>

Office of the Information Commissioner website:

<http://www.informationcommissioner.gov.uk>

Office of the Information Commissioner – guidance notes: Access to pupil’s information held by federations in England

Becta – Good Practice in information handling in federations – keeping data secure, safe and legal and it’s four detailed appendices: (September 2008)

[http://federations.becta.org.uk/upload-dir/downloads/information\\_handling.pdf](http://federations.becta.org.uk/upload-dir/downloads/information_handling.pdf)

[http://federations.becta.org.uk/upload-dir/downloads/information\\_handling\\_impact\\_levels.pdf](http://federations.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf)

[http://federations.becta.org.uk/upload-dir/downloads/data\\_encryption.pdf](http://federations.becta.org.uk/upload-dir/downloads/data_encryption.pdf)

[http://federations.becta.org.uk/upload-dir/downloads/audit\\_logging.pdf](http://federations.becta.org.uk/upload-dir/downloads/audit_logging.pdf)

[http://federations.becta.org.uk/upload-dir/downloads/remote\\_access.pdf](http://federations.becta.org.uk/upload-dir/downloads/remote_access.pdf)

Cabinet Office – Data handling procedures in Government – a final report (June 2008)

[http://www.cabinetoffice.gov.uk/reports/data\\_handling.aspx](http://www.cabinetoffice.gov.uk/reports/data_handling.aspx)

# E-Safety – A Federation Charter for Action

Name of Federation

Name of Local Authority

We are working with staff, pupils and parents / carers to create a federation community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

## Our federation community

Discusses, monitors and reviews our e-safety **policy** on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports **staff** in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole federation curriculum.

Ensures that **pupils** are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the federation's e-safety policy.

Provides opportunities for **parents/carers** to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The federation will report back to parents / carers regarding e-safety concerns. Parents/carers in turn work with the federation to uphold the e-safety policy.

Seeks to learn from e-safety good practice elsewhere and utilises the support of the **LA, SWGfL and relevant organisations** when appropriate.

Chair of Governors

Executive Headteacher

Pupil Representative

## Ideas for federations to consider

To assist federations in drawing up their e-safety policy, SWGfL has issued guidance for federations and a Federation E-Safety Policy Template document. Federations may wish to use the following prompts when

determining and evaluating their policy, which are based on a document contained in the DCSF "Safe to Learn" Overview:

<http://www.teachers.gov.uk/docbank/index.cfm?id=11907>

### Discuss, monitor and review

- Do we hold discussions on e-safety and its definition, involving staff, children and young people, governors and parents?
- Do we keep a record of the incidence of e-safety incidents, according to our agreed definition, and analyse it for patterns – people, places, groups, technologies?
- Do we ask ourselves what makes an e-safe federation?
- What is our federation doing to ensure that our children and young people do not feel vulnerable and are safe to learn, when engaged in online activities?
- Do we celebrate our successes and draw these to the attention of parents/carers and the wider community?

### Support everyone in the federation community to identify and respond

- Do we work with staff and outside agencies to identify all potential forms of e-safety incidents?
- Do we actively provide systematic opportunities for developing pupils' skills to develop safe online behaviour?
- Have we considered all the opportunities where this can be addressed – through the curriculum; through corridor displays; through assemblies; through the Federation Council; through peer support; and through the website and parents' evenings and newsletters?
- Do we ensure that there is support for vulnerable children and young people?
- Do we train all staff to be aware of potential e-safety issues and follow federation policy and procedures on e-safety?
- Do our staff feel adequately supported to be able to respond to and manage e-safety related incidents?

### Ensure that children and young people are aware of how and to whom e-safety incidents should be reported and understand that all e-safety concerns will be dealt with sensitively and effectively

- Do we acknowledge and learn from the high level of skills and knowledge of children and young people in the use of new technologies? (often referred to as the "digital natives")
- Do we regularly canvass children and young people's views on the extent and nature of e-safety issues?
- Do we ensure that young people know how to express worries and anxieties about e-safety?
- Do we ensure that all children and young people are aware of the range of sanctions which may be applied against those involved in e-safety misuse?
- Do we involve children and young people in e-safety campaigns in federation?
- Do we demonstrate that we are aware of the power of peer support? Have we created and publicised schemes of peer mentoring or counselling; buddying or mediation, for example?
- Do we include the phone numbers of help-lines in the federation's student planners?
- Have we made children and young people aware of "how to report abuse"?
- Do we have an e-safety notice board?
- How else do we bring e-safety messages to children and young people's attention?
- What role does our Federation Council already play in our e-safety work? How might that involvement be enhanced?
- Do we offer sufficient support to children and young people who have been involved in e-safety incidents?
- Do we work with children and young people who have been involved, or may be seen as being at risk?

### Ensure that parents/carers are aware of e-safety issues and that those expressing concerns have them taken seriously

- Do we work with parents and the local community to address issues beyond the federation gates that give rise to e-safety issues? – particularly with regard to the possible lack of filtering and monitoring of internet access by children and young people out of federation and with regard to cyber-bullying incidents
- Do parents know whom to contact if they are worried about e-safety issues?
- Do parents know about our complaints procedure and how to use it effectively?

### Learn from effective e-safety work elsewhere and establish effective collaboration

- Have we invited colleagues from a federation with effective e-safety policies and practice to talk to our staff?
- Have we involved local authority staff or other local / regional experts in any way?
- Do we have an established link with the police?

#### Legislation

Federations should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

### Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

### Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

### Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities.

All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

## Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The federation reserves the right to monitor its systems and communications in line with its rights under this act.

## Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

## Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

## Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

## Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

## Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

## Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

## Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

## Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

## Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

## Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the federation context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The federation is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

## The Education and Inspections Act 2006

Empowers Executive Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the federation site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

# Links to other organisations or documents

The following links may help those who are developing or reviewing a federation e-safety policy.

### **SOUTH WEST GRID FOR LEARNING:**

"SWGfL Safe" - <http://www.swgfl.org.uk/safety/default.asp>

### **Child Exploitation and Online Protection Centre (CEOP)**

<http://www.ceop.gov.uk/>

### **ThinkUKnow**

<http://www.thinkuknow.co.uk/>

### **CHILDNET**

<http://www.childnet-int.org/>

## **INSAFE**

<http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

## **BYRON REVIEW (“Safer Children in a Digital World”)**

<http://www.dcsf.gov.uk/byronreview/>

## **Becta**

Website e-safety section - <http://federations.becta.org.uk/index.php?section=is>

Developing whole federation policies to support effective practice:

<http://publications.becta.org.uk/display.cfm?resID=25934&page=1835>

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:

<http://publications.becta.org.uk/display.cfm?resID=32422&page=1835>

“Safeguarding Children in a Digital World”

<http://federations.becta.org.uk/index.php?section=is&catcode=ss to es tl rs 03&rid=13344>

## **LONDON GRID FOR LEARNING**

<http://cms.lgfl.net/web/lgfl/365>

## **KENT NGFL**

<http://www.kented.org.uk/ngfl/ict/safety.htm>

## **NORTHERN GRID**

[http://www.northerngrid.org/ngflwebsite/esafety\\_server/home.asp](http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp)

## **NATIONAL EDUCATION NETWORK**

NEN E-Safety Audit Tool: [http://www.nen.gov.uk/hot\\_topic/13/nen-e-safety-audit-tool.html](http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html)

## **CYBER-BULLYING**

DCSF - Cyberbullying guidance

<http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&productId=DCSF-00658-2007>

Teachernet

<http://www.teachernet.gov.uk/wholefederation/behaviour/tacklingbullying/cyberbullying/>

Teachernet “Safe to Learn – embedding anti-bullying work in federations”

<http://www.teachers.gov.uk/wholefederation/behaviour/tacklingbullying/safetolearn/>

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

East Sussex Council – Cyberbullying - A Guide for Federations:

<https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx>

References to other relevant anti-bullying organisations can be found in the appendix to the DCSF publication “Safe to Learn” (see above)

## **SOCIAL NETWORKING**

Home Office Task Force - Social Networking Guidance -

<http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce>

Digizen – “Young People and Social Networking Services”:

<http://www.digizen.org.uk/socialnetworking/>

Ofcom Report:

[http://www.ofcom.org.uk/advice/media\\_literacy/medlitpub/medlitpubrss/socialnetworking/summary/](http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/)

## **MOBILE TECHNOLOGIES**

“How mobile phones help learning in secondary federations”:

<http://partners.becta.org.uk/index.php?section=rh&catcode=report02a&rid=15482>

Mobile phones and cameras:

[http://federations.becta.org.uk/index.php?section=is&catcode=ss\\_to\\_es\\_pp\\_mob\\_03](http://federations.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03)

## DATA PROTECTION AND INFORMATION HANDLING

Information Commissioners Office - Data Protection:

[http://www.ico.gov.uk/Home/what\\_we\\_cover/data\\_protection.aspx](http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx)

BECTA - Data Protection:

[http://federations.becta.org.uk/index.php?section=lv&catcode=ss\\_lv\\_saf\\_dp\\_03](http://federations.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03)

## PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:

<http://www.iab.ie/>

# Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and federation staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website:

[http://www.swgfl.org.uk/safety/safetyresources.asp?page=federationst\\_resources&audienceid=3](http://www.swgfl.org.uk/safety/safetyresources.asp?page=federationst_resources&audienceid=3)

## Links to other resource providers:

BBC Chatguides: <http://www.bbc.co.uk/chatguide/index.shtml>

Kidsmart: <http://www.kidsmart.org.uk/default.aspx>

Know It All - <http://www.childnet-int.org/kia/>

Cybersmart - <http://www.cybersmartcurriculum.org/home/>

NCH - <http://www.stoptextbully.com/>

Chatdanger - <http://www.chatdanger.com/>

Internet Watch Foundation: <http://www.iwf.org.uk/media/literature.htm>

Digizen – cyber-bullying films: <http://www.digizen.org/cyberbullying/film.aspx>

London Grid for Learning: <http://cms.lgfl.net/web/lgfl/safety/resources>

# Glossary of terms

<b>AUP</b>	Acceptable Use Policy – see templates earlier in this document
<b>Becta</b>	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
<b>CEOP</b>	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes).
<b>CPD</b>	Continuous Professional Development
<b>CYPS</b>	Children and Young Peoples Services (in Local Authorities)
<b>DCSF</b>	Department for Children, Federations and Families
<b>ECM</b>	Every Child Matters
<b>FOSI</b>	Family Online Safety Institute
<b>HSTF</b>	Home Secretary’s Task Force on Child Protection on the Internet
<b>ICO</b>	Information Commissioners Office

<b>ICT</b>	Information and Communications Technology
<b>ICTMark</b>	Quality standard for federations provided by Becta
<b>INSET</b>	In Service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>ISPA</b>	Internet Service Providers' Association
<b>IWF</b>	Internet Watch Foundation
<b>JANET</b>	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
<b>KS1 ..</b>	Key Stage 1 (2, 3, 4 or 5) – federations are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>Learning Platform</b>	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
<b>LSCB</b>	Local Safeguarding Children Board
<b>MIS</b>	Management Information System
<b>MLE</b>	Managed Learning Environment
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to federations across Britain.

**Ofcom** Office of Communications (Independent communications sector regulator)

**Ofsted** Office for Standards in Education, Children's Services and Skills

**PDA** Personal Digital Assistant (handheld device)

**PHSE** Personal, Health and Social Education

**RBC**

Regional Broadband Consortia (eg SWGfL) have been established to procure broadband

connectivity for federations in England. There are 10 RBCs covering 139 of the 150 local

