Ankermoor Primary School

e-safety Policy

(including filtering policy and personal data handling policy)

Adoption Date: See Policy File

Review:

ANKERMOOR PRIMARY SCHOOL

Staffordshire

Contents

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum and Standards Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor – Mrs Julie Dutton. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

See SSCB for further information –

http://www.staffsscb.org.uk/e-SafetyToolkit/Proformas/GgovernorChecklist/

Headteacher and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator Mrs Ella Price
- The Headteacher / Senior Leaders are responsible for ensuring that Mrs Price and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Staff will receive regular monitoring reports from the E-Safety Co-ordinator / Officer as appropriate
- **The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see SSCB website for a flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator / Officer:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / Systems Manager / ICT Technician / ICT Co-ordinator is responsible for ensuring:

- **that the school's ICT infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets the e-safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance**
- **that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed**
- Staffordshire Learning Network provide schools with the RM solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied. Schools are able to control their own permissions and add/amend to the defaults. Staffordshire Learning Technologies can be contacted if schools require assistance with this.
- the school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**
- **they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the E-Safety Co-ordinator**
- **digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level** and only carried out using official school systems – there should be no communication with pupils via external social networking sites
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned 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

Designated person for child protection / Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee

Members of the Curriculum and Standards Committee will assist with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one)

Pupils:

- **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.**
- have a good understanding of research skills
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school **and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school**

Parents / Carers

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

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

Community Users

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

Education – pupils

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

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

- **A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
- Pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems / internet will be posted in the ICT suite 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 school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents evenings

Education - Extended Schools

The school 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:

- **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 school e-safety policy and Acceptable Use Policies**
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / 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 or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- **School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance**
- **There will be regular reviews and audits of the safety and security of school ICT systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**

- **All users will have clearly defined access rights to school ICT systems.**
- **All users will be provided with a username and password**
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)**
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the LA. The school has provided enhanced user-level filtering through the use of the Securus 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 Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SLT (Staffordshire Learning Technologies).
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the curriculum and standards committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place through our AUP for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place via the school office for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- 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 school.
- An agreed policy is in place (to be described) that allows staff to / forbids staff from installing programmes on school 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 school workstations / portable devices. (see School Personal Data Policy Template in the appendix for further detail)
- The school 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 school site unless safely encrypted or otherwise secured. (see School 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 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. Requests for website release should be made on an appropriate request pro-forma.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism, particularly with respect to examination coursework..

Use of digital and video images - Photographic, Video

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

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

Use of Digital / Video Images – Please see in Appendix A at the back of this document updated proformas from County

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 school. These images may then be used in presentations in subsequent lessons.

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

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children. At school events where parents/carers take digital / video images, it is understood that these are solely for personal use and that they must not be uploaded to any media or social networking sites where viewing would be accessible by someone other then the initial user.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

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

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

Signed		Date	

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

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

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

Communications

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

Please identify	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						X	
Use of mobile phones in lessons				X				x
Use of mobile phones in social time	X							
Taking photos on mobile phones or other camera devices				X				X
Use of hand held devices eg PDAs, PSPs	x					X		
Use of personal email addresses in school, or on school network	X							X
Use of school email for personal emails				x				X
Use of chat rooms / facilities				x				X
Use of instant messaging				x				X
Use of social networking sites				X				x
Use of blogs	x				X			

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

- **The official school email service may be regarded as safe and secure and is monitored.** Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.**
- Where possible pupils at KS2 and above will be provided with individual school email addresses for educational use.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate / illegal activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school 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 school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					P
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					P
	adult material that potentially breaches the Obscene Publications Act in the UK					P
	criminally racist material in UK					P
	pornography				P	
	promotion of any kind of discrimination				P	
	promotion of racial or religious hatred				P	
	threatening behaviour, including promotion of physical violence or mental harm				P	
	***any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute**				P	
Using school systems to run a private business					P	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					P	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					P	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					P	
Creating or propagating computer viruses or other harmful files					P	

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				P	
On-line gaming (educational)			P		
On-line gaming (non educational)				P	
On-line gambling				P	P
On-line shopping / commerce			P		
File sharing (in a responsible way)		P			
Use of social networking sites (this excludes our VLE)				P	
Use of video broadcasting eg Youtube	P				

***any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute . . .**

<u>Important Note</u> – staff and pupils are reminded, regardless of the hardware or systems they are using inside or outside school, that information shared electronically that breaches the integrity of the ethos of the school or brings the school into disrepute is unacceptable. If allegations of misconduct as above arise, they will be investigated accordingly and may result in disciplinary action, as detailed in the School's disciplinary procedure

Social networking sites such as 'Facebook' have become extremely popular in recent years. They provide a powerful gateway for communication but they are intended for use by adults (and for use by children 13yrs+ with adult supervision only).

User are reminded of the importance of remaining professional and acting in the best interests of the school at all times. Staff should use social networking sites with due care.

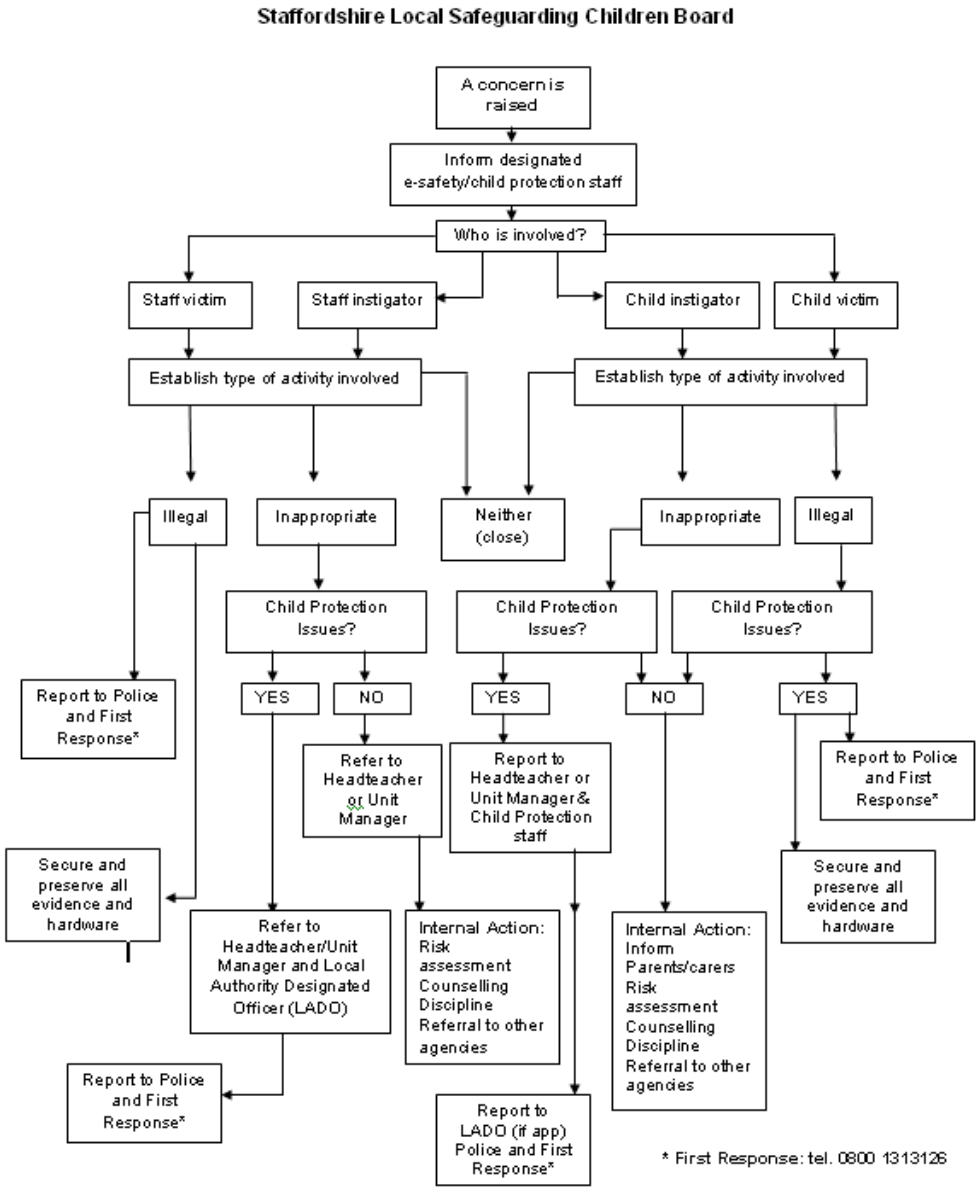
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Misuse includes personal use, where that misuse could bring the school into disrepute. 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 flow chart from the Staffordshire Safeguarding Children's board– below and http://www.staffsscb.org.uk/e-SafetyToolkit/IncidentResponse/ 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 contact the Staffordshire Safeguarding Children's Board

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		P	P	P					
Unauthorised use of non-educational sites during lessons			✓						
Unauthorised use of mobile phone / digital camera / other handheld device			✓						
Unauthorised use of social networking / instant messaging / personal email			✓						
Unauthorised downloading or uploading of files			✓			✓			✓
Allowing others to access school network by sharing username and passwords			✓			✓	✓		✓
Attempting to access or accessing the school network, using another pupil's account (other than with staff permission)			✓			✓	✓		
Attempting to access or accessing the school network, using the account of a member of staff			✓						
Corrupting or destroying the data of other users			✓			✓	✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			✓			✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions			✓			✓	✓		✓

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓	✓		
Using proxy sites or other means to subvert the school's filtering system			✓			✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident			✓			✓			
Deliberately accessing or trying to access offensive or pornographic material			✓			✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓						

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		P	P	P				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓						
Unauthorised downloading or uploading of files		✓						✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓						✓
Careless use of personal data eg holding or transferring data in an insecure manner		✓						
Deliberate actions to breach data protection or network security rules		✓						✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓						✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓					✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓	✓	✓				✓
Actions which could compromise the staff member's professional standing		✓	✓					✓

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓					✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓					✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓						
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓				✓
Breaching copyright or licensing regulations		✓						✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓				✓

Filtering Policy

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 school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the Staffordshire Learning Network schools 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 school's filtering policy will be held by the school's ICT technician. They will manage the school 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 school filtering service must;

- **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 school'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. 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:

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

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

Changes to the Filtering System

At a primary level, changes to the filtering system are rare and will be handled by Mrs Price in consultation with Mr Burns as appropriate.

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 Mrs Price who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at county level, then Mrs Price should contact Staffordshire Learning Technologies with the URL.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Headteacher
- The Curriculum and standards committee
- 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.

Personal Data Handling Policy

Introduction

Schools 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 schools – keeping data secure, safe and legal – Sept 2008).

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

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

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. 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.
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 school 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 school 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 school 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 school's data protection officer is the Headteacher. They will keep up to date with current legislation and guidance and will:

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

The school will identify Information Asset Owners (IAOs) 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

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

Display equipment must be positioned so that the screen display is not visible to any unauthorised persons.

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 school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the school 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 annually. Parents / carers of young people who are new to the school will be provided with the fair processing notice through an induction pack.

A copy of a specimen fair processing notice can be found at: **http://www.teachernet.gov.uk/management/ims/datamanagement/fpnpupils/**. It contains a relevant wording for the regulations pertaining to the transfer of information to Connexions, in secondary schools and new requirements resulting from the introduction of ContactPoint. A new specimen FPN is available for 2008/9. Schools are advised to contact their Local Authority for local versions of the Fair Processing Notice.

Training & awareness

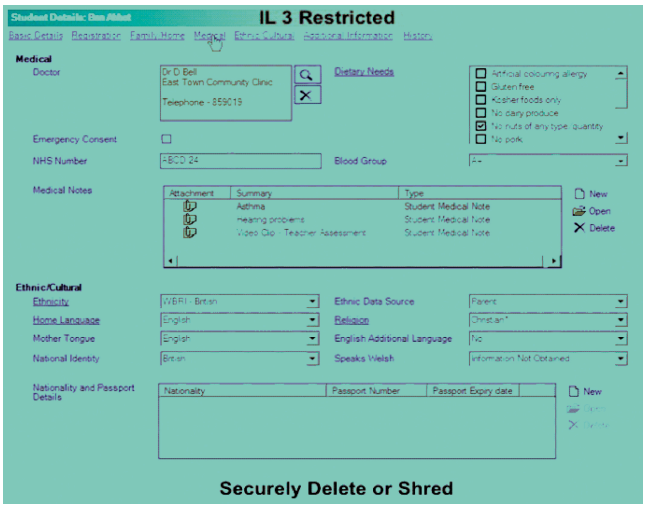
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

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

Identification of data

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



Impact levels are as follows:

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

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

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

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

Secure Storage of and access to data

The school 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. 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 school equipment (this includes computers and portable storage media). 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 school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

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

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests 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 school

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

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- 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.

Disposal of data

The school 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, 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.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

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.

Legislation

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

Standard Photography and Video Consent Form

Name of School: .

Name of Pupil: . **Class: .**

Name of Parent/Guardian: .

The school confirms that it shall only use photographic images of your child in line with its Code of Practice.

A copy of the school's Code of Practice is printed on the reverse of this form.

Please tick the relevant boxes and sign below in all instances where you give your consent for photographic images of your child being used. In some instances your child may also be named alongside their photograph.

	I agree to my child's image being used: ***(please tick)***
In school materials aimed at the school community	
On the school web site	
In Staffordshire County Council materials – this may include printed materials and filming	
On the Staffordshire County Council web site	
In media coverage of the school	

I confirm that I have read and agree to the terms contained within this Consent Form.

Signature: . **Date:**

(Parent/Guardian)

Draft

Code of Practice

This code of conduct specifies the manner in which ……School will use and make available photographic images of pupils.

The school will:

1. Not use photographs in any form of internal or external publication where we do not have consent or there is written objection from a parent/guardian
2. Not use photographs of pupils in PE clothes or swimwear other than for instructional purposes where images are needed to demonstrate the activity to pupils.
3. Not reveal within the image personal details, such as pupils' date of birth, home address or telephone number.

In using materials of school age children for its purposes the County Council will:

1. Always ensure that parental permission has been given via this standard form.

2. Not use images of children to illustrate child protection issues, fostering and adoption services or Youth Offending Services.