

# Bilbrook Church of England Middle School

## E-Safety Policy and Procedures

May 2010

### Contents

<b>Part 1: Policy</b>	Page
1A; Introduction: background and scope of the policy	2
1B: Development, monitoring and review	4
1C: Roles and responsibilities	5
1D Statement of procedures	7

<b>Part 2: Statement of procedures</b>	Page
2A: Education and training	8
2B: Technical information	10
2C: Password procedures	11
2D: Curriculum	13
2E: Use of digital and video images	14
2F: Data protection	15
2G: Communications	16
2H: Unsuitable, inappropriate & illegal activities	18
2I: Responding to incidents of misuse	20

<b>Part 3: Appendices</b>	Page
3A: Photography and video consent form	24
3B: Use of Images Code of Practice	25
3C: Pupil Acceptable Use Policy Agreement	26
3D: Staff and Volunteer Acceptable Use Policy Agreement	29
3E: Parent/Carer Acceptable Use Policy Agreement	31
3F: Legislation	32
3G: RM Internet Filtering Policy	35

# Part 1: Policy Statement

## 1A: Introduction

### Background

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

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

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

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

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

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

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

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

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

## **Scope of the policy**

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

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

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

Members of staff are also subject to the Staffordshire County Council's *Code of Conduct for Employees*, and teachers are subject to the General Teaching Council's *Code of Conduct and Practice for Registered Teachers*.

## **1B: Development, monitoring and review**

This E-Safety Policy has been developed by the school's leadership team and the school governors. Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- Governors' committees
- School website and newsletters

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

## **1C: 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 Staffing and Curriculum Committee receiving regular information about e-safety incidents and monitoring reports on e-safety issues. The nominated Governor for Child Protection will take on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular discussions with the Headteacher, who is the school's Child Protection Officer
- regular reporting to the governors

### **Headteacher and leadership team**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher and the leadership team are responsible for ensuring that they receive relevant suitable continuing professional development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as appropriate.
- The Headteacher and leadership team, comprise the E-Safety Committee in this school, and are responsible for internal monitoring and action on e-safety matters.
- The Headteacher and at least one other member of the leadership team are 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**

The E-Safety Coordinator in this school is the designated person for child protection.

The E-Safety Coordinator:

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

### **Network Manager**

The Network Manager is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- 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
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the RM solution 'Safety Net Plus' is installed (through Staffordshire Learning Network) and is implemented.
- the school's RM filter is applied, monitored, updated and upgraded as necessary.
- he/she keeps up to date with e-safety technical information in order to effectively carry out the e-safety role and to inform and update others as relevant.
- the use of ICT in school is regularly monitored and updated using both the RM filter and the Securus software in order that any misuse or attempted misuse can be reported to the E-Safety Committee for investigation, action and sanction as appropriate.

### **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 school's current E-Safety Policy and practices
- they have read, understood and signed the school's Staff Acceptable Use Policy (AUP) and Agreement
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation, action and sanction as appropriate.
- digital communications with pupils (through, for example, email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school's policy for e-safety and acceptable use
- 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; this includes the use of RM Tutor
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held electronic devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use, and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Designated Person for Child Protection**

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

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

### **E-Safety Committee**

Members of the E-safety Committee (in this school, the school's senior leadership team) will be responsible for the production, review and monitoring of the school's E-Safety Policy, and related documents and procedures.

### **Pupils**

All pupils in the school:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held electronic 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 and Carers**

Parents and 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 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 Acceptable Use Policy agreement (AUP), before being provided with access to school systems.

## **1D: Statement of Procedures**

In turning this policy into practice, there will be a statement of procedures which will be regularly reviewed as part of the process of development, monitoring and review:

Part 2 of this document describes the procedures in the school relating to the following areas:

- Education
- Technical information
- Password policy
- Curriculum
- Use of digital and video images
- Data protection
- Communications
- Unsuitable, inappropriate & illegal activities
- Responding to incidents of misuse

## Part 2: Statement of Procedures

This section describes the procedures in the school relating to the following areas:

- 2A Education and training
- 2B Technical information
- 2C Password procedures
- 2D Curriculum
- 2E Use of digital and video images
- 2F Data protection
- 2G Communications
- 2H Unsuitable, inappropriate, illegal activities
- 2I Responding to incidents of misuse

### 2A: Education and Training

#### Pupils

Whilst regulation and technical solutions are very important in minimising e-risk, 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-risks and build their resilience.

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

- A planned e-safety programme is provided as part of ICT, PSHE and other lessons as appropriate and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and other pastoral activities as appropriate.
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of information.
- Pupils are helped to understand the need for the pupil Acceptable Use Policy agreement (AUP) and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet are posted in all rooms and displayed on log-on screens.
- Staff act as good role models in their use of ICT, the internet and mobile devices.

#### Parents and carers

Parents and carers may 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 may either underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about what they would do about it. "*There is a generational digital divide.*" (Byron Report).

The school therefore seeks to provide information and awareness to parents and carers through letters, newsletters, the school website, VLE, and parents' evenings.

#### Extended Schools

If needs arise, the school offers 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 are also 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.

#### Staff training

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

- A planned programme of formal e-safety training is made available to staff. An audit of the e-safety training needs of all staff is 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 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 receives regular updates through attendance at county training sessions and by reviewing guidance documents released by BECTA, the county and others.
- This e-safety policy and its updates are presented to and discussed by staff at staff meetings and training sessions.
- The E-Safety Coordinator provides advice, guidance and training to individuals as required.

### **Governor training**

Governors take part in e-safety training and awareness sessions, with particular importance for those who are members of any group involved in ICT, health and safety, and safeguarding. This may be offered in a number of ways including:

- 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.

## 2B: Technical information

### Infrastructure and equipment; filtering; monitoring

The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within the E-Safety Policy are implemented. In this school, the county's Staffordshire Learning Technologies (SLT) service is contracted to manage the school's ICT network.

The school adopts the following procedures to ensure that the people with the relevant roles named in the above sections will be effective in carrying out their e-safety responsibilities.

- School ICT systems are 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 are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the Network Manager and are reviewed, at least annually, by the E-Safety Committee.
- All users are provided with a username and password by the Network Manager who keeps an up to date record of users and their usernames. Users are required to change their password every month.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager and the ICT Coordinator are available to the Headteacher and kept in the school safe.
- Users are 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 RM. RM has its own *Internet Filtering Policy* (see Appendix 3G) which the school approves.
- The school has provided enhanced user-level filtering through the use of the RM filtering programme.
- In the event of the Network Manager or the ICT Coordinator needing to switch off the filtering for any reason, or for any user, this is logged and carried out by a process that is agreed by the headteacher.
- Any filtering issues are reported immediately to RM.
- Requests from staff for sites to be removed from the filtered list are considered by the Network Manager and the ICT Coordinator. If the request is agreed, this action is recorded and logs of such actions are reviewed regularly by the E-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools including RM Tutor are used by staff to control workstations and view users' activity in the ICT suites.
- An appropriate system is in place for users to report any actual or potential e-safety incident to the Network Manager or the ICT Coordinator.
- 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 system is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) on to the school system.
- An agreed procedure is in place regarding the downloading of executable files by users: the downloading of such files is not permitted and is not possible on our system.
- An agreed procedure is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (See Section 2F).
- As part of the E-Safety Policy, staff are not permitted to install programmes on school workstations and portable devices. The network does not allow such installations to take place. The only people able to install programmes are the Network Manager and the ICT Coordinator.
- An agreed procedure is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. (See Section 2F)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## **2C: Password procedures**

### **Introduction**

The school will be responsible for ensuring that the school 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 school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

### **Responsibilities**

The management of the password security procedure will be the responsibility of the Network Manager and the ICT Coordinator.

All users (adults and young people) will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the Network Manager and the ICT Coordinator. Any changes carried out are notified to the manager of the password security procedures.

Users will change their passwords every term.

### **Training / Awareness**

It is essential that users are made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss.

Members of staff and other adult users will be made aware of the school's password procedures:

- at induction
- through the school's E-Safety Policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password procedures:

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

### **Statement of Procedures**

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

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

The following rules apply to the use of passwords:

- passwords must be changed every term
- the password should be, where possible, a non dictionary word
- the password should include three of – uppercase character, lowercase character, number, special character
- passwords are not to be displayed on screen, and are securely hashed (use of one-way encryption)
- requests for password changes should be authenticated by the Network Manager or the ICT Coordinator to ensure that the new password can only be passed to the genuine user.

Where sensitive data is in use – particularly when accessed on laptops – those laptops need to be accessed by a password.

The “master / administrator” passwords for the school ICT system, used by the Network Manager and the ICT Coordinator must also be available to the Headteacher and kept in a secure place ( school safe). The school does not allow one user to have sole administrator access.

### **Audit / Monitoring / Reporting / Review**

The Network Manager 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 the E-Safety Committee at regular intervals (at least termly).

These procedures will be regularly reviewed (at least annually) in response to changes in guidance and evidence gained from the logs.

## **2D: Curriculum**

**E-safety is a focus in all areas of the curriculum. Staff are expected to reinforce e-safety messages in the use of ICT across the curriculum.**

- In lessons where internet use is pre-planned, it is best practice that pupils are 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 (refer to section on infrastructure and equipment; filtering; monitoring).
- Where pupils are allowed to freely search the internet, eg using search engines, staff are required to be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager or ICT Coordinator temporarily remove those sites from the filtered list for the period of study. Any request to do so must be audited with clear reasons for the need. Records of such requests and actions are maintained.
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of information
- Pupils are 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.

## **2E: Use of digital and video images (photos and videos)**

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 indefinitely 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.

### **School use of images**

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they 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 pupils are published on the school website.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

### **Images taken by parents/carers at school events for personal use**

- Photographs and videos may be taken on the basis that they are for private retention and not for publication in any manner, including use on personal websites.
- The school reserves the right to withdraw this permission in any specific circumstance.

*See Appendices 3A and 3B for use of permission template for digital and video images.*

## 2F: 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/or 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 procedures (see below) once it has been transferred or its use is complete

## 2G Communications

This is an area of rapidly developing technologies and uses.

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:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
1 Mobile phones may be brought to school	✓				✓			
2 Use of mobile phones as part of the planned curriculum (refer also to item 4)		✓					✓	
3 Use of mobile phones in social time	✓							✓
4 Taking photos of pupils on personal mobile phones or other personal camera devices				✓				✓
5 Use of hand held devices eg PDAs, PSPs, DSs, as part of the planned curriculum		✓					✓	
6 Use of personal email addresses in school, or on school network		✓						✓
7 Use of school email for personal emails in non teaching time and in personal breaks	✓							✓
8 Use of public chat rooms / facilities*				✓				✓
9 Use of public instant messaging*				✓				✓
10 Use of public social networking sites*				✓				✓
11 Use of public blogs/wikis*				✓				✓

\*Non-public use of these facilities is included on the school's learning platform and use of these facilities within the SLN2 is acceptable.

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 pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored

- Users must immediately report, to the E-Safety Coordinator , 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 pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils are provided with individual school email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## 2H 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 are 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. The school policy restricts certain internet usage as follows:

<b>User Actions</b>		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<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					X
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
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				X		
<b>Using school systems to run a private business</b>					X	
<b>Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Local Authority and / or the school</b>					X	
<b>Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions</b>					X	

## User Actions

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
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				X	
On-line gaming (educational)			X		
On-line gaming (non educational) (in line with rules under Communication)				X	
On-line gambling (in line with rules under Communication)				X	
File sharing (in line with rules under Communication)			X		
Use of social networking sites (in line with rules under Communication)			X		
Use of video broadcasting eg Youtube (in line with rules under Communication)			X		

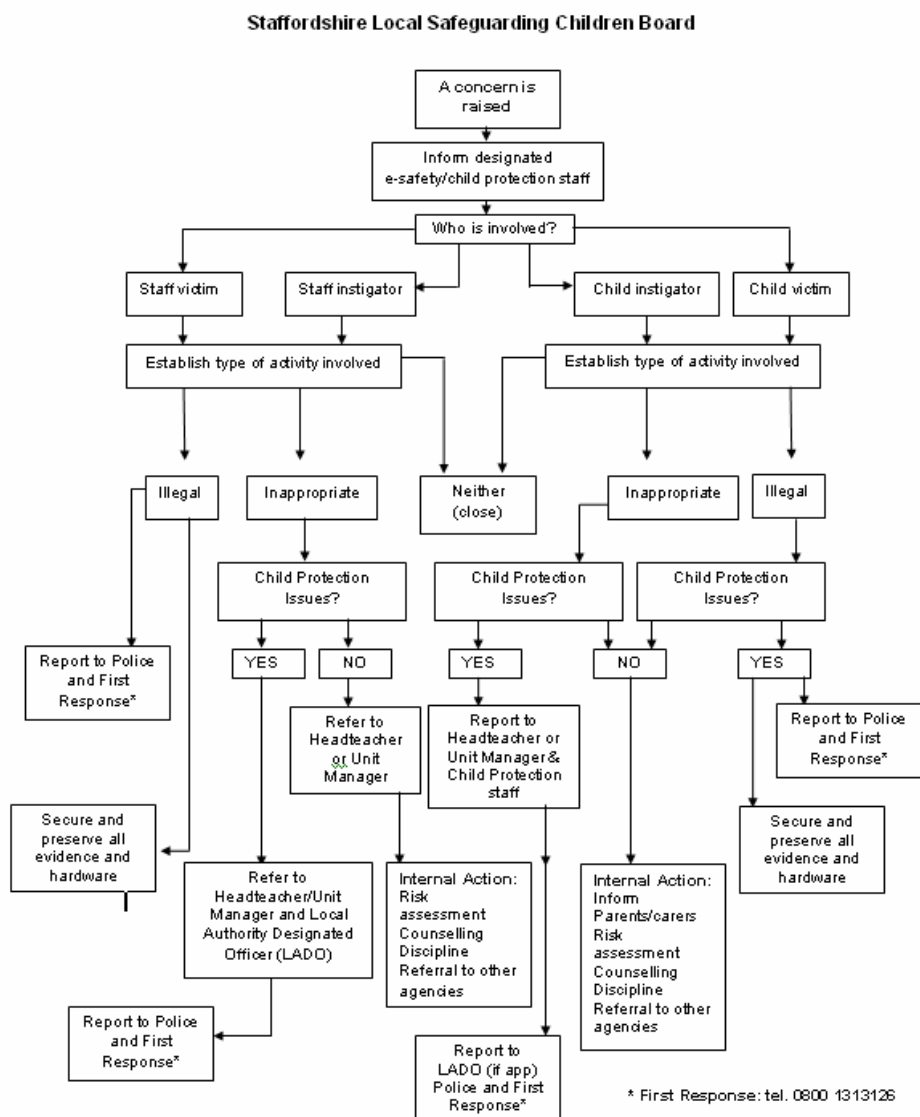
## 2I Responding to incidents of misuse

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

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

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- 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/> will 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 Staffordshire Safeguarding procedures will be followed.

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

## **Pupils**

### **Possible incidents**

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other handheld device
- Unauthorised use of social networking / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

### **Actions/sanctions**

The actions and sanctions listed below will be followed according to the individual incident, its nature, severity, and whether it is a repeated offence:

- Refer to class teacher
- Refer to head of department or a member of the school's leadership team
- 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, isolation, exclusion

## **Members of staff**

### **Possible incidents**

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data eg holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with 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

**Actions/sanctions**

The actions and sanctions listed below will be followed according to the individual incident, its nature, severity, and whether it is a repeated offence:

- 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

## **Part 3:Appendices**

- 3A Photography and video consent form
- 3B Use of Images Code of Practice
- 3C Pupil Acceptable Use Policy Agreement
- 3D Staff and Volunteer Acceptable Use Policy Agreement
- 3E Parent/Carer Acceptable Use Policy Agreement
- 3F Legislation
- 3G RM Internet Filtering Policy

**BILBROOK CE MIDDLE SCHOOL  
PARENTAL CONSENT FORM**

**USE OF PHOTOGRAPHIC IMAGES**

Please PRINT the following information:

Name of pupil \_\_\_\_\_

Name of parent/carer \_\_\_\_\_

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

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

**Please tick the boxes and sign below in all instances where you give your consent for photographic images of your child being used and/or named.**

	Agree to use of image	Agree to my child being named
In school materials aimed at the school community		
On the school website		
In Local Education Authority materials		
On the LEA website		
In the media coverage of the school		

**Use of photographic images**

- The school will not use images of pupils without the written consent of a parent/carer
- Primarily photographs of children will be as part of a group
- Pupils will not be photographed in swimwear
- Pupil images will only include the name and age of the child with parental permission
- At school events, photographs and videos may only be taken on the basis that they are for private retention and are not for publication in any manner.

The school confirm that it will only use photographic images of your child in line with this code of practice and in order to demonstrate or promote activities relating to the school's curricular or extra curricular provision.

SIGNED \_\_\_\_\_ Parent/carer

Date \_\_\_\_\_

**Bilbrook CE Middle School  
Use of Images Code of Practice**

*Wherever photographs are mentioned in this document, this should be read to include still, video and electronic images.*

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

The school may wish to use images of children in a number of situations, including the following:

- Newspapers and magazines, to give media coverage to events such as sports days, concerts, fund raising, special events
- Television, for instance local and national news stories, documentaries
- The school prospectus
- The school website

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/carer
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.

*NB: Photographs and images taken by parents/carers at school events for personal use: The governors give consent for photographs to be taken on the basis that they are for private retention and not for publication in any manner, including use on personal websites and social networking sites. This consent may be withdrawn in certain circumstances.*

# Pupil Acceptable Use Policy (AUP) Agreement

## School Policy

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

*This Acceptable Use Policy is intended to ensure:*

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

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

## Acceptable Use Policy Agreement

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

*For my own personal safety:*

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- 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 school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

*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.
- In my use of ICT I will show respect for the school and the school community.

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

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are part of the school's learning platform.

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

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

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

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

## Pupil Acceptable Use Agreement Form

This form relates to the 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 school ICT systems.

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

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

Name of Pupil

Group / Class

Signed

Date

### Staff (and Volunteer) Acceptable Use Policy (AUP) Agreement

#### School Policy

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

*This Acceptable Use Policy is intended to ensure:*

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

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

#### Acceptable Use Policy Agreement

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

*For my professional and personal safety:*

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

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

- I will 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 school'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 school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use public chat and social networking sites in school unless I have responsibility within the e-safety policy for monitoring the use of the school's ICT systems.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

*The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the*

*smooth running of the school:*

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

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school. I understand that I may not make use of the school's ICT facilities (including my laptop) for the purpose of running a private business.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer

Signed

Date

## Parent / Carer Acceptable Use Policy (AUP) Agreement

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

*This Acceptable Use Policy is intended to ensure:*

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- 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 school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

### Permission Form

Parent / Carers Name

Pupil Name

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

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

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

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

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

Signed

Date

### 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 event 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 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 pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.