Margaret McMillan Primary School

E-safeguarding Policy

Content

Background / Rationale

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

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

The requirement to ensure that children 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-safeguarding 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 head teacher 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-safeguarding policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

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

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

This policy has been adapted from that provided by the South West Grid for Learning. Copies of the original document can be found here [Adobe Acrobat Reader or Microsoft Word]

Development / Monitoring / Review of this Policy

This e-safeguarding policy has been developed by a working group made up of:

- Senior Leadership Team (with joint responsibility for child protection issues)
- ICT Coordinator
- ICT Technician

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

- Staff meetings
- Governors' Joint Operations Committee (JOC)

Schedule for Monitoring & Review

This e-safeguarding policy was approved by the Governing Body / Governors Sub Committee on:	June 2010
The implementation of this e-safeguarding policy will be monitored by the:	Senior Leadership Team, ICT Coordinator, ICT Technician
Monitoring will take place at regular intervals:	Termly meeting between Deputy Head, ICT Coordinator and ICT Technician
The E-safeguarding Policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safeguarding or incidents that have taken place.	Reviewed by full Governing Body; 22 May 2012
Should serious e-safeguarding incidents take place, the following external persons / agencies should be informed:	LADO Safeguarding Officer / Police

The school will monitor the impact of the policy using:

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

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers, 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-safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles & Responsibilities

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

Governors:

Governors are responsible for the approval of the E-safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the JOC receiving regular information about e-safeguarding incidents and monitoring reports. The Safeguarding Governor has taken on responsibility for e-Safeguarding. Their role will include reporting to relevant Governors committee / meeting.

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safeguarding) of members of the school community, though the day to day responsibility for e-safeguarding will be delegated to the E-safeguarding Co-ordinator / Officer.
- The Head teacher / Senior Leaders are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safeguarding role and to train other colleagues, as relevant.
- The Head teacher / 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-safeguarding monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular, termly monitoring reports from the ICT Co-ordinator.
- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safeguarding allegation being made against a member of staff.

Senior Leadership Team:

- Takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safeguarding incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safeguarding incidents and creates a log of incidents to inform future e-safeguarding developments.
- Attends relevant meeting / committee of Governors

ICT Coordinator / ICT Technician:

The 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
- The school meets the e-safeguarding technical requirements outlined by the Child Exploitation and On-Line Protection Centre (see http://ceop.police.uk/publications/).
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- The Local Authority is informed of issues relating to the filtering applied by the Grid
- The school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- He / she keep up to date with e-safeguarding technical information in order to effectively carry out their e-safeguarding role and to inform and update others as relevant
- 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 Senior Leadership Team for investigation / action / sanction
- Monitoring software / systems are implemented and updated.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safeguarding matters and of the current school e-safeguarding 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 ICT Coordinator or Senior Leader Team for investigation / action / sanction
- Digital communications with pupils should be on a professional level and only carried out using the school's Virtual Learning Environment (VLE).
- e-Safeguarding issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school e-safeguarding and acceptable use policy
- Pupils click to accept terms of use (including details of e-safeguarding) every time they log in to the VLE.
- 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-safeguarding issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated persons for child protection

These Named Persons are trained in e-safeguarding 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

(N.B. it is important to emphasise that these are child protection issues, not technical issues - the technology simply provides additional means for child protection issues to develop.)

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. At Foundation Stage (FS) and Key Stage One (KS1) it would be expected that parents / carers would sign on behalf of the pupils.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying. This would be confirmed through signature of the Pupil Acceptable Use Policy.

- Should understand the importance of adopting good e-safeguarding practice when using digital technologies out of school and realise that the school's E-safeguarding 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-safeguarding campaigns / literature. Parents and carers will be responsible for:

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

Policy Statements

Education – Pupils

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

- A planned e-safeguarding 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. The first ICT lesson of each half-term will cover elements of e-safeguarding.
- Key e-safeguarding messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens

Education – parents / carers

Many parents and carers have only a limited understanding of e-safeguarding 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 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 and leaflets
- VLE
- Parents information meetings

Education - Extended Schools

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.

Training – Staff

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

- Regular training on-site and through LA courses will be made available to staff.
- Teachers will receive e-safeguarding training as part of their annual safeguarding CPD.
- All new staff members receive e-safeguarding training as part of their induction programme, ensuring that they fully understand the school e-safeguarding policy and Acceptable Use Policies
- The Senior Leadership Team will receive regular updates from the LA and by reviewing guidance documents released by BECTA / LA and others.
- This E-safeguarding policy and its updates will be presented to and discussed by staff in staff meetings.

Training – Governors

Governors should take part in e-safeguarding training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safeguarding / 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-safeguarding responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safeguarding technical requirements outlined by CEOP.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the E-safeguarding Committee (or other group).
- All users (at KS2 and above) will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Users will be required to change their password every 90 days (staff) or year (pupils). Users in KS1 and Foundation Stage will use group or class log-ons and passwords, but staff members have been made aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access. A school password policy template is provided in the appendix to this document)
- The “administrator” passwords for the school ICT system, used by the ICT Technician must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the Local Authority.
- In the event of the ICT Technician 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 Head teacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the Local Authority.

- 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 for users to report any actual / potential e-safeguarding incident to the SLT.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. Trainee or supply teachers will be given a user name and password to be used for that day (supply1, supply2 and supply3). The ICT Technician shall keep a record of the teacher's name and the user id allocated for the day. This ID should have access to the school's resources folder, the internet and other resources applicable to their teaching. They will not be given access to folders containing assessment details or other personal information.
- Users should not download executable files from the internet without first speaking to the ICT Technician (or ICT Coordinator if the Technician is unavailable).
- An agreed policy 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. Further details are contained in the Staff Acceptable Use Policy.
- An agreed policy is in place that details rules for staff regarding installing programmes on school workstations / portable devices. Further details can be found in the Staff Acceptable Use Policy.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices. Further details can be found in the Staff Acceptable Use Policy.
- The school infrastructure and individual workstations, including staff laptops, are protected by up to date virus software, with updates downloaded from the internet automatically, as soon as they become available.

Curriculum

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

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Wherever possible, the children should be given hyper-links to click on rather than a website to type in.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Staff should also carry out searches using the relevant search terms immediately prior to the lesson, to check that no inappropriate content (including adverts) is returned in the search.
- Safe search should be used in the classroom with children.
- 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.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

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 e.g. on social networking sites.

- Staff members 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 (this is covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

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

- 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.

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 anti-virus software installed on all computers and laptops will prevent any known viruses or mal-ware being transferred onto the school network
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

	Staff & other adults				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						X
Taking photos on mobile phones or own camera devices				X				X
Use of hand held devices eg PDAs, PSPs (provided by school)	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 (VLE only)	X				X			
Use of social networking sites				X				X
Use of blogs (on VLE only)	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 should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications can 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 pupils or parents / carers must be professional in tone and content. These communications may only take place on the VLE. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils in KS2 will be provided with internal school email addresses for educational use – these cannot be used outside of school.
- 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 activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					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	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Education Bradford and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (e.g. 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 e.g. role-playing games)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing					X	
Use of social networking sites (other than through VLE)					X	
Use of video broadcasting to upload files to the internet e.g. Youtube					X	

Responding to incidents of misuse

It is expected 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, irresponsible or, very rarely, deliberate misuse. Listed on the following two pages are the responses that will be made to any apparent or actual incidents of misuse:

Apparent or actual misuse which appears to involve illegal activity could include:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct or activity

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. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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

Pupils

Actions / Sanctions

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

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	RRefer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Management Instruction	Disciplinary action (including suspension where appropriate
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X						
Unauthorised downloading or uploading of files	X					X	
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		X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X					
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X					X
Actions which could compromise the staff member's professional standing		X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X
Using proxy sites or other means to subvert the school's filtering system		X					X
Accidentally accessing offensive or pornographic material and failing to report the incident		X					X
Deliberately accessing or trying to access offensive or pornographic material		X	X				X
Breaching copyright or licensing regulations	X						
Continued infringements of the above, following previous warnings or sanctions		X					X

Acknowledgements

Margaret McMillan Primary School would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-safeguarding Policy:

- The SWGfL E-safeguarding Group and the SWGfL E-safeguarding Conference Planning Group, on whose template this document has been based.
- CEOP
- DCSF
- Becta
- Byron Review – Children and New Technology – “Safer Children in a Digital World”

Appendices

Can be found on the following pages:

- Pupil Acceptable Use Policy Agreement
- SMART rules
- Staff and Volunteers Acceptable Use Policy Agreement
- Parents / Carers Acceptable Use Policy Agreement
- School Filtering Policy
- School Password Security Policy
- School E-safeguarding Charter
- Legislation
- Resources
- Glossary of Terms

Pupil Acceptable Use Policy Agreement

I understand that I must use school ICT systems responsibly, so that there is no risk to my safety or to others.

For my own personal safety:

- I understand that the school will check my use of the ICT systems
- I will treat my username and password like my toothbrush – I will not share it, and will not try to use any other person's username and password.
- I will follow the "SMART rules", when I am on-line.
- I will not share personal information about myself or others when on-line.
- I will not arrange to meet people that I have talked with on-line.
- I will immediately report to a trusted adult anything I am uncomfortable with that I see on-line.

When I use the school network, including the internet:

- I will use the systems for learning and not for personal use.
- I will not download or upload any files to the internet except, with permission, to the school's website.

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

- I will respect others' work and will only open/delete /save my own files.
- I will be polite and responsible when I communicate with others, and will not use inappropriate language.
- I will not take or share images of anyone without their permission.

To help keep the school ICT system safe:

- I will not use my personal devices (mobile phones / USB devices etc) in school.
- I will report any damage or faults with ICT to my teacher.
- I will not save, or try to install programmes on a machine.
- I will not alter computer settings.
- I will only use discussion forums within the school's VLE.
- I understand that there are consequences if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school where they involve my membership of the school community (e.g. cyber-bullying, use of images or personal information).

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

Signed

Date

Class

Be Smart on the Internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Teacher Record of the Pupil Acceptable Use Agreement Form

Pupils will only be allowed to use ICT systems in school once they have signed and returned their pupil acceptable use policy. Please complete annually and display in your classroom.

Name	Form signed and returned

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and children in today's society, both within schools and in their lives outside school. The internet and other forms of ICT 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.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff members 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 educate the children in my care in the safe use of ICT and embed e-safeguarding in my work with children.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, 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. Where these images are published (e.g. 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 chat and social networking sites in school, with the exception of those available through the VLE (or those directly related to teaching – e.g. TES or The Key).
- I will only communicate digitally with pupils and parents / carers using the VLE. 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:

- I understand the confidential nature of school emails and documents and will ensure that I maintain the security of my school account on any devices I use (personal or school).
- I will not use personal email addresses on the school ICT systems, during school hours.
- 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 the school network, or store programmes on a computer, nor will I try to alter computer settings. If I need to install or download a programme, I will email the ICT Technician at least 3 working days in advance, to allow time for him to carry out the work.
- I can install software on my school laptop provided this has been acquired legally.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action 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 Name

Signed

Date

Parent / Carer Acceptable Use Policy Agreement

Computers have become integral to the lives of children and children, both in and out of school. Forms of ICT such as the internet are powerful tools, which open up new opportunities for effective learning. Children should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Children are responsible users and stay safe while using the internet and other forms of ICT.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of e-safeguarding and are involved in the education and guidance of children 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, in return, expects the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, to inform you of the school expectations of the children 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 child to have access to the internet and to ICT systems at school.

I know that my child has signed an Acceptable Use Agreement and the school provides e-safeguarding 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 to protect children when they use the internet and ICT systems. However, 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 child'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-safeguarding.

Signed Date

Use of Digital / Video Images

The use of digital photographs and video images plays an important part in learning activities. Pupils and members of staff may use digital cameras and videos 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.

We will ensure that when images are published that the children 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.

Permission Form

Parent / Carers Name	
Pupil Name	
Class	

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child. 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.

Signed _____ Date _____

School Filtering Policy

Introduction

As a member of the Bradford Learning Network, the school automatically receives a filtered broadband service, with some flexibility for changes at local level. This service is intended to prevent users accessing material that is illegal and / or inappropriate in an educational environment. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. It is 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.

Responsibilities

The responsibility for the day-to-day management of the school's filtering policy will be held by the ICT Co-ordinator and the ICT Technician. They will manage the school filtering, in line with this policy and will keep records 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
- Made to a member of the SLT, who will then pass the request to the ICT Technician once approval has been given.
- Reported to the E-safeguarding Governor every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to SLT 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 will be made aware of the importance of filtering systems through the e-safeguarding education programme, with e-safeguarding lessons held regularly throughout the year, and posters and displays being in place in the ICT room and classrooms. 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 Policy and through the VLE.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to SLT who will decide whether to make school level changes (as requested). If it is felt that the site should be filtered (or unfiltered) at Bradford Learning Network level, the ICT Technician should phone the relevant Local Authority service.

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-safeguarding Policy and the Acceptable Use agreement.

Audit / Reporting

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

- SLT
- JOC
- Safeguarding Governor
- 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.

School Password Security Policy

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 policy will be the responsibility of the ICT Technician.

All users (adults and young people) from KS2 upwards will have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security. The password should be changed annually, in September. All users in FS and KS1 will use a class user ID.

Passwords for new users and replacement passwords for existing users can be allocated by the ICT Technician. Upon receiving a start date for a new pupil, the school administrator should pass the child's name, year group and class to the Technician, who will then be able to set up a network account and a VLE account for the child prior to their starting at the school.

Staff members will change their passwords every 120 days.

Training / Awareness

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

- Induction
- The school's e-safeguarding policy and password security policy
- The Acceptable Use Agreement

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

- In ICT and / or e-safeguarding lessons
- Through the Acceptable Use Agreement

Policy Statements

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

All users (at KS2 and above) will be provided with a username and password by the ICT Technician who will keep an up to date record. (Until Sep 2010 only Y5 and Y6 will have passwords. This will be extended to lower KS2 from Sep 2010).

The following rules apply to the use of passwords:

- Passwords must be changed every 120 days (adults) or one year (pupils)
- The last four passwords cannot be re-used
- The password should be a minimum of 3 characters long
- The account should be "locked out" following six successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Requests for password changes should be made directly to the ICT Technician to ensure that the new password can only be passed to the genuine user

- The ICT Technician will keep of record of user ids which have been reset, and will report excessive requests to the SLT every term.

The “administrator” passwords for the school ICT system, used by the ICT Technician must also be available to the Head teacher or other authorised senior leader and kept in a secure place (e.g. school safe).

Audit / Monitoring / Reporting / Review

The ICT Technician 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 SLT at regular, termly intervals.
This policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

Further reading

Teachernet – Data processing and sharing -
http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/

Office of the Information Commissioner website:
http://www.informationcommissioner.gov.uk

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

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

http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf

http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf

http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf

http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf

http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf

Cabinet Office – Data handing procedures in Government – a final report (June 2008)
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

E-safeguarding – A School Charter for Action

Name of School	Margaret McMillan Primary School
Name of Local Authority	Bradford

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

Our school community:

- Discusses, monitors and reviews our e-safeguarding policy on a regular basis.
- Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safeguarding across the whole school curriculum.
- Ensures that pupils are aware, through e-safeguarding education, of the potential e-safeguarding risks associated with the use of ICT and mobile technologies, that all e-safeguarding concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safeguarding policy.
- Provides opportunities for parents/carers to receive e-safeguarding education and information, to enable them to support their children in developing good e-safeguarding behaviour. The school will report back to parents / carers regarding e-safeguarding concerns. Parents/carers in turn work with the school to uphold the e-safeguarding policy.
- Seeks to learn from e-safeguarding good practice elsewhere and utilises the support of the LA, Bradford Learning Network and relevant organisations when appropriate.

Chair of Governors	
Head teacher	
Pupil Representative	

Legislation

Schools should be aware of the legislative framework under which this E-safeguarding 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 Head teachers, 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.

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Becta
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1 ..	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safeguarding programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

Margaret McMillan
Primary School
Inspiration • Aspiration • Determination

www.mmps.bradford.sch.uk