E-Safety Policy
Responsible person – Assistant Head
Next scheduled review – Summer 2019

Date	Reviewed by	Amended (Y/N)
Autumn 2013	Written by Debbie Hanson	Yes
Spring 2015	Debbie Hanson	No
Autumn 2015	Sarah Billingham / Mel Banner	Yes
Autumn 2016	Sarah Billingham / Mel Banner	Yes
Summer 2017	Sarah Billingham	Yes
Summer 2018	Sarah Billingham	Yes
Summer 2019		

This policy was agreed by governors on (insert date)

Meath School

E-Safety Policy

Mission Statement

We work to create a calm supportive learning environment where high standards of behaviour and conduct are expected from all members of the school community.

Introduction

The E-Safety committee is delegated by the Principal to lead on all matters relating to E-Safety.

This document builds upon what is considered to be the best and most effective practice and provides a formal structure within which this practice may be implemented consistently and fairly. It is designed to ensure consistency of application in encouraging respect for others, rewarding positive attitudes, good behaviours and a positive environment for everyone.

The pupils at Meath School present with severe and complex speech, language and communication needs (including Aspergers Syndrome learners) that affect, to varying extents, their ability to understand and use language effectively for all communication. This can also affect their understanding of the correct way of communicating and the meaning of communication.

It is therefore essential that staff appreciate the difficulties a pupil may have in understanding what is expected of them and coping with the frustrations of their communicative needs. We must also recognise the communicative importance of all behaviours whether they conform or not. For some pupils, a lack of understanding of unwritten rules mean they require a highly structured approach to achieve acceptable standards of behaviour. It can also mean that it is difficult for our pupils to understand that other people would want to cause them harm or not be telling the truth which can make them extremely vulnerable.

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- 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 social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents/carers, friends and the wider community) to be aware and to assist in this process.

Our school's e-safeguarding policy has been written taking into account Surrey Guidelines.

Policy and leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

Responsibilities: The E-Safety committee

Meath School has an E-Safety committee led by our E-Safety Manager – Sarah Billingham, Assistant Principal and made up of Mel Banner, E-Safety Coordinator, Debbie Hanson, Residential Services Manager ,Sheila Shanks, PA to Head of School and Annabel Bates, Governor and meets on a termly basis to:

- Review and monitor this E-Safety policy.

- Consider any issues relating to school filtering

- Discuss any E-Safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Surrey Safeguarding Children Board (SSCB).

Responsibilities: E-Safety Manager

Our E-Safety Manager is the person responsible for reporting to the Principal and governors for the day to day issues relating to E-Safety.

- Chairs E-Safety committee meetings

- attends relevant meetings and committees of Governing Body

- reports regularly to Senior Leadership Group (SLG)

- has been DCPO trained

E-Safety Coordinator

The E-Safety Coordinator with members of the committee:

- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident

- provides training and advice for staff

- 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 with E-Safety Manager and governor to discuss current issues, review incident logs and filtering change control logs

- receives appropriate training and support to fulfil their role effectively

- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

- maintains a current record of all staff, volunteers, pupils and visitors who are granted access to use the system

- has been CEOP trained

Responsibilities: Governors

Our governors are responsible for the approval of this policy. The governors (or a governors' subcommittee) receive regular information about E-Safety incidents and monitoring reports. A member of the governing body has taken on the role of E-Safety governor which involves:

- regular meetings with the E-Safety Manager and Co-ordinator with an agenda based on:

- monitoring of E-Safety incident logs

- monitoring of filtering change control logs

- monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices

- reporting to relevant Governors committee / meeting

Responsibilities: Principal

- The Principal is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety is delegated to the E-Safety Co-ordinator and the committee

- The Principal and another member of the senior management team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff; see flow chart on dealing with E-Safety incidents – below and relevant HR / disciplinary procedures)

Responsibilities: Classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices

- they have read, understood and signed the school's Acceptable Use Policy for staff

- they report any suspected misuse or problem to the E-Safety Co-ordinator

- digital communications with students (email / social media software /voice) should be on a professional level and only carried out using official school systems

- E-Safety issues are embedded in the curriculum and other school activities.

Responsibilities: ICT Technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack, security will be reviewed regularly

- users may only access the school's networks through a properly enforced password protection policy

- shortcomings in the infrastructure are reported to the ICT Coordinator or Principal so that appropriate action may be taken.

- all internet access has age appropriate filtering provided by a recognised filtering system which has been checked to ensure that it is working, effective and reasonable

- has responsibility for blocking / unblocking internet sites in the school's filtering system

- the school uses recognised internet provider

- the network has virus and anti spam protection

Policy development, monitoring and review

This E-Safety policy has been developed by a working group made up of the E-Safety Committee.

- School E-Safety Coordinator

- Senior Leaders

- Teachers

- School Support Staff

- ICT Technical staff

- Governors (especially the E-Safety governor)

Schedule for development / monitoring / review of this policy

The implementation of this E-Safety policy will be monitored by the:	The E-Safety committee under the direction of the E-Safety Coordinator

Monitoring will take place at regular intervals:	Annually
The governing body will receive a report on the implementation of the E-Safety policy generated by the monitoring group (which will include anonymous details of E-Safety incidents) at regular intervals:	Termly
The E-Safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next anticipated review date will be:	Spring Term 2019
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	Surrey Safeguarding Children Board E-Safety representative Surrey Police

Policy Scope

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 Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the 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-Safety behaviour that take place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.
Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers agreement for their child/ren to use ICT systems)
- Community users of the school's ICT system

Acceptable use policies are revisited and re-signed annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents/carers.

For children in EYFS and KS1 parents/carers may sign on behalf of their children
Staff and volunteers sign when they take up their role in school and in the future if
significant changes are made to the policy

Parents/carers sign once when their child enters the school. The parents' policy also
includes permission for their child to use the schools ICT resources (including the
internet) and permission to publish their work. A copy of the pupil AUP is made available
to parents/carers at this stage and at the beginning of each year.

Community users sign when they first request access to the school's ICT system.

Induction policies for all members of the school community include this guidance.

Self Evaluation

Evaluation of E-Safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent/carer, teachers …) are taken into account as a part of this process.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT Policies:

ICT Policy	How ICT is used, managed, resourced and supported in our school
E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using ICT. The E-Safety policy constitutes a part of the ICT policy.

Other policies relating to E-Safety:

Anti-bullying	How our school strives to illuminate bullying – link to cyber bullying
PSHE	E-Safety has links to this – staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. The E-Safety policy forms a part of the school's safeguarding policy
Behaviour	Linking to positive strategies for encouraging E-Safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

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 (illegal - The Protection of Children Act 1978)**

- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**

- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**

- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (Public Order Act 1986)**

- pornography

- promotion of any kind of discrimination

- promotion of racial or religious hatred

- threatening behaviour, including promotion of physical violence or mental harm

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

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business

- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by I CAN and / or the school

- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)

- Creating or propagating computer viruses or other harmful files

- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

- On-line gambling

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.
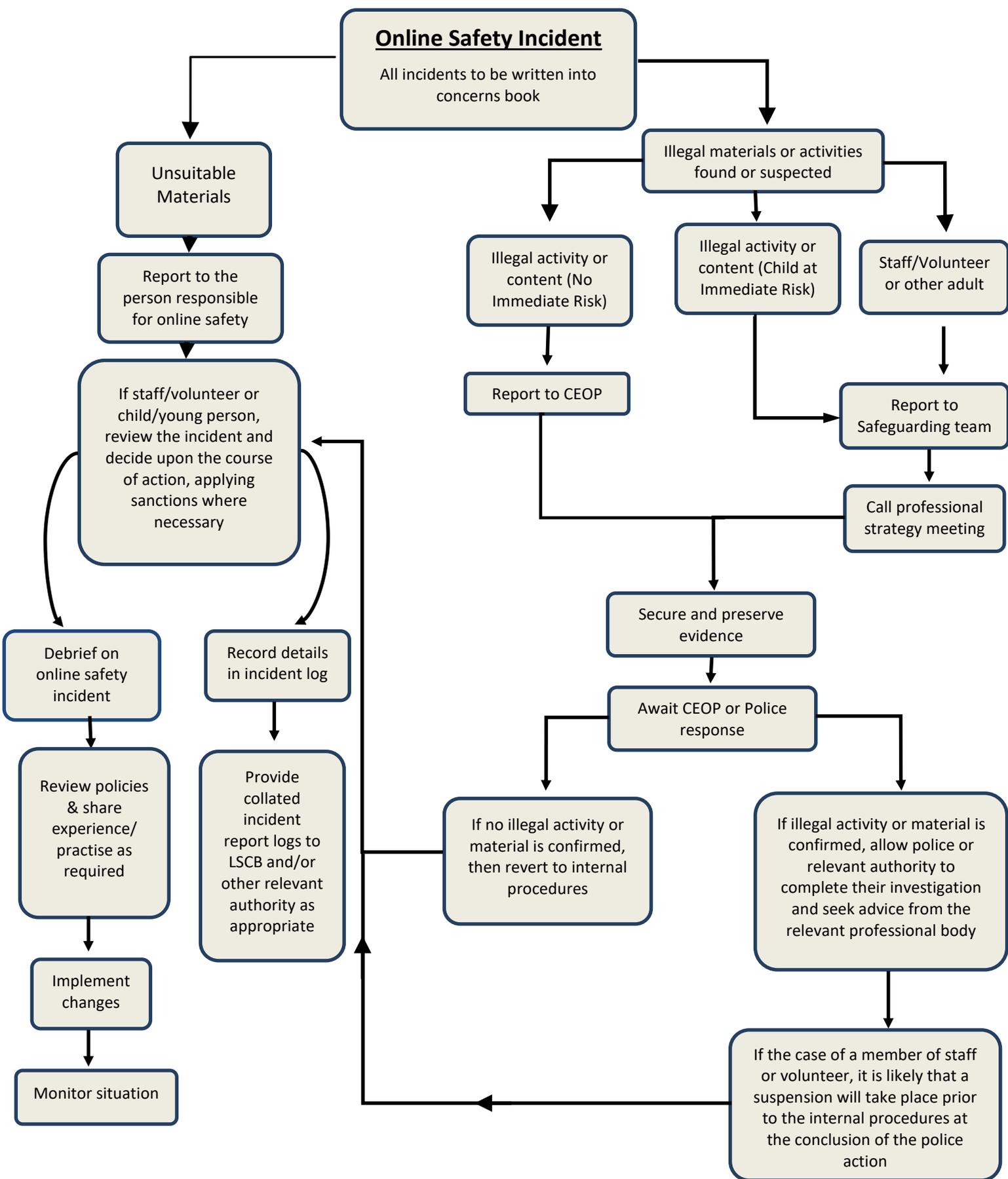
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil sanctions	Refer to class teacher	Refer to E-Safety	Refer to Principal	Refer to Police	Refer to E-Safety	Inform parents / carers	Removal of network /	Warning	Further sanction e.g.
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 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	☐	☐	☐		☐	☐	☐	☐	

Staff sanctions

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

Online Safety Incident

All incidents to be written into concerns book

Unsuitable Materials

Report to the person responsible for online safety

If staff/volunteer or child/young person, review the incident and decide upon the course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies & share experience/ practise as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal activity or content (No Immediate Risk)

Report to CEOP

Illegal activity or content (Child at Immediate Risk)

Staff/Volunteer or other adult

Report to Safeguarding team

Call professional strategy meeting

Secure and preserve evidence

Await CEOP or Police response

If no illegal activity or material is confirmed, then revert to internal procedures

If illegal activity or material is confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

If the case of a member of staff or volunteer, it is likely that a suspension will take place prior to the internal procedures at the conclusion of the police action

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 belo[...] [...] made to any apparent or actual incidents of misuse:

All incidents to be written into the concerns book kept.

Audit / Monitoring / Reporting / Review

The E-Safety Coordinator will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Principal / and a governor on a termly basis.

Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
    - o Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
    - o Members of staff are free to use these devices in school, outside teaching time.(away from the children)
- Pupils are not currently permitted to bring their personal hand held devices into school. If any hand held devices are brought into school they will be locked away in the front office.

Email

Access to email is provided for all users in school

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services 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

- Pupils have access to an individual email account for communication within school.

- A structured education programme is delivered to pupils which help them to be aware of the dangers of and good practices associated with the use of email.

- Staff may only access personal email accounts outside of child contact time.

- Users must immediately report, to their class teacher / 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.

- Incoming email from an unknown source must be treated as suspicious and attachments not opened.

Videoconferencing

Videoconferencing equipment is used in the Residential Department and must be switched off when not in use and not set to auto answer.

External IP addresses should not be made available to other sites.

Videoconferencing contact information should not be put on the school Website.
Only web based conferencing products that are authorised by the school are permitted for classroom use.

Videoconferencing is normally supervised by a member of staff. In the event of this not being the case pupils should ask permission from the supervising member of staff before making or answering a videoconference call.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in schools and only where it is granted may children participate.

Only key administrators have access to videoconferencing administration areas.

Use of digital and video images

- 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.

- Members of staff are allowed to take digital still and 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 captured using 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

- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section for guidance on publication of photographs

Use of web-based publication tools

Our school uses the public facing website, www.meathschool.org.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).

- Only pupil's first names are used on the website, and only then when necessary.

- Detailed calendars are not published on the school website.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - Annual written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Digital Literacy and Closed Social Media

Class teachers monitor the use of closed social media by pupils regularly in all areas, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the school administrator and the ICT technician.

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to a closed social media or email tool.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to closed social medial for the user may be suspended.

d) The user will need to discuss the issues with a member of SLG before reinstatement.

e) A pupil's parent/carer may be informed.

A visitor may be invited onto closed social by the administrator (usually the computing Coordinator) following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the **Teachers' Standards** as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf). Teachers translate these standards appropriately for all matters relating to E-Safety.

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 technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

Filtering

Introduction

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

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **ICT Technician** (with ultimate responsibility resting with the **Principal**). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible we will:

- be logged in change control logs
- be authorised by a second responsible person prior to changes being made (this will normally happen anyway, as part of the process and will be the member of staff who originally made the request for the change).

All users have a responsibility to report immediately to class teachers / E-Safety Coordinator/PA to Principal any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

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 are made aware of the importance of filtering systems through the school's E-Safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the AUP (a part of their induction process)

- briefing in staff meetings, training days, memos etc. (from time to time and on-going).

Parents/carers will be informed of the school's filtering policy through the Acceptable Use Agreement and through E-Safety awareness sessions / newsletter etc.

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.

Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to

- the E-Safety governor

- the E-Safety committee

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

E-Safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

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

- A planned E-Safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

- We use the resources on CEOP's Think U Know site as a basis for our E-Safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2) Focus provided by Rigby's Rising Stars

- Key E-Safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises as well as through safer internet day activities.

- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. This can be facilitated using Kids Search.

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address)
    - Cross checking references (can they find the same information on other sites)
    - Checking the pedigree of the compilers / owners of the website
    - See lesson 5 of the Cyber Café Think U Know materials below

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils are taught how to make best use of internet search engines to arrive at the information they require

- We use the resources on CEOP's Think U Know site as a basis for our E-Safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Pupils play a part in contributing to this policy through the school council.

Staff training

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

- A planned programme of formal E-Safety training will be made available to staff. An audit of the E-Safety training needs of all staff will be carried out regularly.

- It is expected that some staff will identify E-Safety as a training need within the performance management process.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and acceptable use policies which are signed as part of their induction
- The E-Safety Coordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents released by the DfE, local authority, the SSCB and others.
- The E-Safety Committee will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governor training

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

- Attendance at training
- Participation in school training / information sessions for staff or parents/carers

The E-Safety governor works closely with the E-Safety Coordinator and reports back to the E safety committee. The E safety governor reports back to the full governing body on a termly basis.

Parent and carer awareness raising

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

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Wider school community understanding

The school will offer family learning courses in ICT, media literacy and E-Safety so that parents/carers and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents/carers. 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.

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

Equality and Inclusion

At Meath School we will continuously seek to ensure that all members of the school community are treated with respect and dignity. Every individual will be given fair and equal opportunities to develop their full potential regardless of their gender, ethnicity, cultural and religious background, sexuality, disability or special educational needs and ability, and other factors as detailed within the school's Equality Policy. These meet in full the requirements of the Equality Act, October 2010.

MEATH SCHOOL

Acceptable use policy agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

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 will, where possible, educate the young people in my care in the safe use of ICT and embed E-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (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 in the E-Safety policy.

- I will not disclose my username or password to anyone else, nor will I try to use anyone else'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

images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will not use social networking to make friends with pupils/parents/carers and will not share information relating to the children.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and I CAN have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the E-Safety policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- My personal mobile ICT devices will be password protected.

- I will not use personal email addresses when working with the children

- 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 (see e-security policy).

- 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 Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- Images of pupils/staff will only be stored/used in line with the data protection policy and with parent/carer/staff consent.

- 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 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. This could involve a warning, a suspension, referral to HR and in the event of illegal activities the involvement of the police.

- I understand that it is a criminal offence to use school ICT systems for a purpose not permitted by its owner.

- I understand that I must adhere to the requirements of the GDPR.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

MEATH SCHOOL

Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users 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 ICT (especially the internet).

- 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 them to agree to be responsible users.

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

Child's name	
Parent/Carer's name	
Parent/Carer's signature:	
Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), 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.

Parent/Carer's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's virtual learning environment (VLE)

As the parent / carer of the above child I give my permission for this activity.

Parent/Carer's signature:	
Date:	

Your agreement of consent will carry through the school. If your circumstances change it is your responsibility to inform the school.

Our school's E-Safety Policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

MEATH SCHOOL

Acceptable use policy agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to agree to this acceptable use policy.

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 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, of which I become aware, to a member of the school's staff.

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.

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 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 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.

28

- 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, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT system being withdrawn.

Community user Name:	
Signed:	
Date:	

Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following

  - Internal response or discipline procedures

  - Involvement by Local Authority or national / local organisation (as relevant).

  - Police involvement and/or action

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

  - incidents of 'grooming' behaviour

  - the sending of obscene materials to a child

  - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to

these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Sample documents for recording the review of and action arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template: http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.

- There is information about the site's authors (about us, our objectives, etc.)

- There is a contact for further information and questions concerning the site's information and content.

B. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?

- easy to navigate through the site - links are clearly marked etc?

- have working links?

- Have inappropriate adverts?

C. CONTENT - Is the website's content meaningful in terms of its educational value?

- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.

- The site promotes equal and just representations of racial, gender, and religious issues.

- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.

- The site does not link to other sites which may be harmful / unsuitable for the pupils

- Is the website current?

D. ACCESSIBILITY - Is the website accessible?

- Loads quickly?

- Does the site require registration or passwords to access it?

- The site does not require usage fees to be paid.

Relevant legislation:

Education Act 1996

Education and Inspections Act 2006

Education Act 2011 Part 2 (Discipline)

The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012

Health and Safety at Work etc. Act 1974

Obscene Publications Act 1959

Children Act 1989

Human Rights Act 1998

Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.