Moor Green Primary Academy

E-Safety Policy

DRAFT V2: Approved by ESafety Committee, 20 April 2015
Amendments made after consultation period for staff and parents ending May 8 2015

E&OE
Due for ratification by Governors

Moor Green E-Safety Policy

Contents

Moor Green Primary School E-Safety Policy

Moor Green Primary School E-Safety Policy

Moor Green Primary School E-Safety Policy

Introduction
Pages: 2

Introduction

Overview

- This document replaces the policy that was initially written in May 2008 by Rachel Hill, Ruth Garner and Peter Kaye and was last reviewed in July 2012.

- The policy has been written using guidance materials from the South West Grid for Learning (SWGfL), a leading organisation in E-Safety Education in the UK.

- The school has a new E-Safety Curriculum in place from September 2014, developed by the SWGfL. It was considered prudent to adopt the guidance of the SWGfL regarding E-Safety policy, in order to maintain consistency between policy and practice and to ensure breadth and depth of coverage.

Aims of the policy

- To enable all Moor Green pupils, staff and community members to be responsible, respectful, competent, confident and creative users of Information Technology, both within and outside school

- To safeguard pupils, staff and community users against threats of abuse

- To protect the security and integrity of the school's and Academy Trust's ICT infrastructure

Development of the Policy

This E-Safety policy has been developed with a whole-school approach, using guidance materials from the SWGfL. Consultation with the whole school community has taken place through a range of formal and informal meetings. The final draft of the policy was drawn up by the school's E-Safety Committee in May 2015.

The policy is awaiting ratification by governors. An interim governing body is currently in place.

Moor Green Primary School E-Safety Policy

Introduction

Pages: 2

Schedule for Development/Monitoring/Review

This E-Safety policy was approved by the Governing Body on:	*Insert date*
The implementation of this E-Safety policy will be monitored by the:	E-Safety Committee
Monitoring will take place at regular intervals:	Once per term
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:	Once per term
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:	July 2016 2016
Should serious E-Safety incidents take place, it may be necessary to inform the following external agencies :	Academy Trust, Police, CEOP

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
- Samples of work from ESafety lessons
- Feedback from pupils in class discussions and School Council meetings
- Surveys/questionnaires of
    - pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of the school community who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers/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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

E-Safety at Moor Green: An Overview of Provision

What is E-Safety?

E-Safety is concerned with the safe and responsible use of technology and the internet. This includes, but is not limited to, personal computers, tablets, mobile phones, and gaming devices.

Ofsted have identified 3 areas of risk regarding online activity:

- Inappropriate **contact**
  - E.g. abusive messages, explicit photographs, requests to meet,
- Inappropriate **conduct**
  - E.g. uploading dangerous material such as viruses, phishing, hacking, breaching or attempting to breach firewalls and filters
- Inappropriate **content**
  - E.g. violence, strong language, explicit images, gambling
  -

Recently a 4th 'C' has been added to the list: **commercialism**. This relates to the increasing trend for advertising and marketing online, such as adverts alongside YouTube videos, 'pop-up' adverts on websites, and in-app purchases in games

E-Safety Provision

At Moor Green we have both proactive and reactive approaches to E-Safety for pupils, staff and parents, as outlined below:

Proactive: Educate	ESafety and Digital Literacy Curriculum CPD for staff, through taught sessions and self-study resources Assemblies Workshops 'Hector' Button SWGfL Boost 'Whisper' Tool E Leaders (peer supporters in KS2) Information on VLE and website Twitter and blog devoted to ESafety Multi-lingual resources available in reception and online
Raise awareness Build resilience Encourage responsibility Facilitate communication and reporting	
Reactive: Respond	'Hector' button Boost 'Whisper' Tool In-house reporting proformas SWGfL Boost Incident Reporting Toolkit
Record incidents Report if necessary Support those affected Review	

Further details of how these approaches will be implemented will be found in the relevant sections of the policy.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the Computing and E-Safety Coordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (See Policy Statement: Responding to incidents of misuse, page 18)
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about E-Safety incidents and monitoring reports. The role of the E-Safety Governor will include:

- liaising with the E-Safety Coordinator
- representation of the Governing Body on the E-Safety Committee
- monitoring of E-Safety incident logs
- monitoring of filtering/change control logs
- reporting to relevant Governors

Child Protection/Safeguarding Designated Person(s)

Should be trained in E-Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

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

E-Safety Coordinator

- leads the E-Safety committee
- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- provides training and advice for staff
- liaises with relevant outside agencies (e.g. Academy Trust, CEOP)
- liaises with technical staff (e.g. Network Birmingham)
- receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of the Governing Body
- reports regularly to Senior Leadership Team

E-Safety Committee

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding E-Safety. The Committee will also be responsible for regular reporting to the Governing Body.

Members of the E-Safety Committee will assist the E-Safety Coordinator with:

- the production, review and monitoring of the school E-Safety policy and related documents
- mapping and reviewing the E-Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and pupils about E-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

For further details see Appendix 4: E-Safety Committee Terms of Reference, page 46

Network Manager/Technical staff

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required E-Safety technical requirements and any other relevant E-Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leadership Team/ E-Safety Coordinator for investigation/action/sanction as appropriate.
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher or E-Safety Coordinator for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current 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.

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through, for example, parents' meetings and workshops, literature, website, 'MG Connect' site and information about national and local E-Safety campaigns. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/VLE
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems/website/VLE as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems. (See Appendix 13: Acceptable Use Agreement for Community Users, page 62)

Policy Statements: Education and Training for the School Community

Education and Training: Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach.

The growing use of mobile devices and social media exposes young people to additional risks beyond school. Because the school cannot monitor or control the use of mobile devices and social media outside the school, it has a duty to educate pupils to recognise and avoid E-Safety risks, to develop a respectful and responsible attitude online, and build resilience, whether in or outside school.

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-Safety curriculum will be provided as part of Computing, PHSE and other lessons and will be regularly revisited. The school currently uses the E-Safety Curriculum produced by the South West Grid for Learning (SWGfL) and Common-Sense Media (see E-Safety and Digital Literacy Curriculum Document.) A summary of this curriculum is available on the school website and VLE for parents.
- Key E-Safety 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 online 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
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- 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, staff should be vigilant in monitoring the content of the websites the young people visit.

- The home page on all workstations accessed by pupils is Swiggle, a search engine featuring a safe search facility, online safety advice and educational links provided by the SWGfL. This enables pupils to search safely, promotes important E-Safety messages and provides an easy route to access E-Safety resources. http://www.swiggle.org.uk/Home

- Children should be taught how and why to use the 'Hector' button (a tool on their workstations which enables them to block any inappropriate content) and the 'Whisper' tool (an online reporting form which they can use to log incidents of bullying, inappropriate content, or any other E-Safety concerns.)

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Parents should be encouraged to take an active role in their children's E-Safety education. (See next section.)

Education and Training Parents/Carers

The school will provide information and awareness about ESafety to parents and carers through:

- Curriculum activities
- Letters, newsletters, leaflets, web site, VLE
- Parents/carers evenings/
- Workshops
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g.
  www.swgfl.org.uk
  www.saferinternet.org.uk/
  http://www.childnet.com/parents-and-carers

Education: The Wider Community

In the long term, the school will endeavour to provide opportunities for local community groups/members of the community to gain from the school's E-Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website hosting E-Safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their E-Safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk)

Education and Training: Staff/Volunteers

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy (See Policy Statement: Teaching and Support Staff). Training will be offered as follows:

- A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. 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 Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL/Link2ICT/CEOP other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Training: Governors

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

- Attendance at training provided by CEOP/ National Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons.)

Policy Statement: Communications

	Staff & other adults				Pupils			
A wide range of rapidly developing communications technologies has the potential to enhance learning. This table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages. **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[1]						x[2]	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x[3]							x
Taking photos on mobile phones			x[4]					x
Use of other mobile devices e.g. tablets, gaming devices		x[5]					x[6]	
Use of personal email addresses in school, or on school network		x[7]						x
Use of school email for personal emails				x				x
Use of messaging apps		x						x
Use of social media		x[8]					x	

[1] Staff mobile phones should be placed in a locker during teaching time and switched off or on silent.
[2] Pupils who bring mobile phones to school must leave them, switched off or on silent, at the office when they arrive at school and collect them at the end of the day.
[3] Staff should avoid having mobile phone conversations in public areas such as the staffroom. This is both to safeguard their own privacy and to avoid distracting others.
[4] On some occasions staff may need to take photographs to upload to the school's Social Media sites. This is allowed, with the permission of the ESafety co-ordinator, as long as the photographs do not feature children.
[5] Only devices owned by the school or otherwise approved by the Esafety Coordinator may be used during lessons.
[6] Occasionally pupils will be allowed to bring in devices from home, for example as part of a class treat or at the end of term. In such cases, devices must be labelled with each pupil's name and must be locked away securely when not in being used. Pupils may not access the school's internet service on their own devices.
[7] Personal email addresses may be used as a last resort if the school email service in not functioning. Staff should inform the Computing and Esafety Coordinator in such an event.
[8] There are many potential benefits to using applications such as Twitter to enhance teaching and learning. Staff should inform the Computing and ESafety Coordinator before using any social media applications in lessons.

Use of blogs	x						x	

Moor Green Primary School E-Safety Policy

Policy Statement: Communications

Pages: 2

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

- The official school email service, currently using Microsoft's Office 365 and Outlook, may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access). An exception may be made in the event of the school service malfunctioning, in which case staff may use personal email addresses. Staff should notify the Computing and E-Safety Coordinator in such an event.
- Users must immediately report, to the Computing and E-Safety Coordinator and/or Head Teacher, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**.**
- 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 social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils may email staff and vice-versa but pupils may not email each other or send emails to external email addresses. Measures are in place within the email system to facilitate this.
- If a teacher wishes to establish email contact between their pupils and a specific external organisation or individual, for example an author or another school, they should consult the ESafety Coordinator for advice on best practice and to allow contact.
- Pupils should be taught about the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official school email addresses should be used to identify members of staff.
- When using social media and blogs with pupils, teachers should liaise with the Computing and E-Safety Coordinator to discuss best practice.

Policy Statement: Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- They do not comment publicly on media coverage regarding the school unless with the permission of the Head Teacher. This includes, but is not limited to, comments on Facebook, Twitter and online versions of newspapers and magazines. Commenting can leave individuals vulnerable to harassment from the public and/or media organisations.
- Personal opinions should not be attributed to the school or local Academy Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. It is recommended that staff do not have public profiles on Facebook in order to protect personal and professional identity and integrity.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Policy Statement: Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:		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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				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	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					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	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Online gaming (both educational and non-educational)[9]			X			
Online gambling					X	
Online shopping/commerce					X	
File sharing using platforms other than the school's Office 365 system					X	
Use of social media			X			
Use of messaging apps					X	
Use of video broadcasting e.g. YouTube			X[10]			

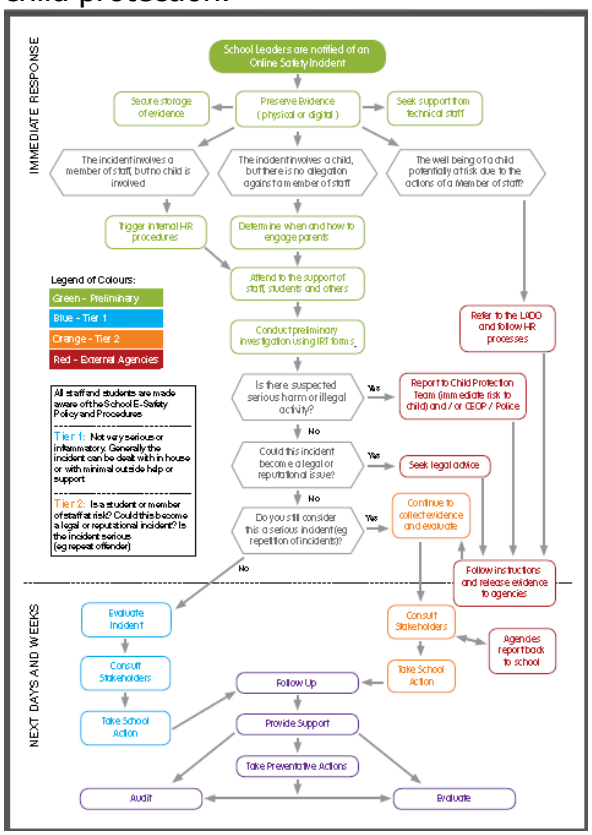
[9] Pupils may only play games that have been approved by an adult.
[10] YouTube can be used by teachers for lessons providing content has been vetted beforehand. Pupils should not use YouTube due to the risk of viewing inappropriate content and/or comments.

Policy Statement: Responding to incidents of misuse

Introduction

This guidance is intended for use when staff need 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 involve illegal or inappropriate activities.

The flowchart in Appendix 11, page 64 is taken from the SWGfL's Incident Response Tool, (IRT) part of their BOOST ESafety service package to which the school subscribes. The IRT has been drawn up with guidance from lawyers and experts in child protection.



In the event of an ESafety Incident taking place, the member of staff involved should complete an ESafety Incident Report Log (See Appendix 15: E-Safety Incident Reporting Log, page 65) and return it as soon as possible to the ESafety Co-ordinator. The ESafety Co-ordinator will then make a judgement as to how to deal with the incident, following guidance laid out in the Incident Response Tool.

Following the guidance in the Incidence Response Tool will ensure consistency of practice and will ensure that all stakeholders – including victims – are treated fairly and sensitively.

The Incident Response Tool is an interactive PDF document that is regularly updated online. The flowchart in Appendix 11 is a simplified version of the process. A paper copy of the IRT is available in the ESafety file in the staffroom. Paper copies of the flowchart are on display in the Staffroom and ICT room.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- 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. It is recommended that a laptop be used to cover for this eventuality. 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/Academy Trust 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
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school and 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.

School Actions & Sanctions

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

Pupils	**Actions/Sanctions**								
Incidents:	Refer to class teacher	Refer to C/E-S Coordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction 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							X	
Unauthorised use of mobile phone/digital camera/other mobile device	X	X	X			X		X	
Unauthorised use of social media/ messaging apps/personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X			X	X		X	
Allowing others to access school network by sharing username and passwords	X	X	X		X	X		X	
Attempting to access or accessing the school network, using another student's /pupil's account	X	X	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 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	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	

Staff	Actions/Sanctions									
Incidents: NB Details in this section are still TBC and will need to be confirmed by the Governing Body.	Refer to line manager	Refer to C/E-S Coordinator	Refer to Headteacher Principal	Refer to Academy Trust/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	C/E-S Coordinator /HT to discuss with staff member	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).			X			X				
Inappropriate personal use of the internet/social media /personal email		X				X	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	X			X		X		
Careless use of personal data e.g. holding or transferring data in an insecure manner							X			
Deliberate actions to breach data protection or network security rules		X	X			X		X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X			X		X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X		X		
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with 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 's filtering system			X			X				
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X					X		
Breaching copyright or licensing regulations		X					X			
Continued infringements of the above, following previous warnings or sanctions	X	X	X					X		

Policy Statement: Use of Digital and Video Images

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers 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. Example: NSPCC: Using photographs of children for publication

http://www.nspcc.org.uk/Inform/research/briefings/Photographing-children_wda96007.html

- 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. See Appendix 10: Use of Digital/Video Images Page 56

Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that 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
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice
- The managed service provider is fully aware of the school E-Safety Policy, Acceptable Use Agreements and other policies, and acts in line with them.

Responsibilities

The management of technical security will be the responsibility of the Network Manager and the school's Computing Leader.

Policy statements

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 ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- All users will have clearly defined access rights to school technical systems.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see Password section below).
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Mobile device security and management procedures are in place.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place (see Appendix 15: E-Safety Incident Reporting Log page 65) for users to report any actual/potential technical incident to the E-Safety Coordinator/Network Manager.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
    - The user will need to firstly read and sign the appropriate Acceptable Use Agreement (either Staff/Volunteer or Community Users.)
    - Upon completion of the Agreement, the Computing and E-Safety Coordinator will assign a username and temporary password.
    - The user must change their password upon their first login.
    - When the user no longer requires access (e.g. in the case of student teachers, when their placement ends), the Computing and E-Safety Coordinator will delete the user from the system.
- An agreed policy is in place regarding the extent of personal use that staff and family members are allowed on school devices that may be used out of school:
    - The device must be signed out of school with the approval of the Computing and E-Safety Coordinator and must be used in accordance with the Acceptable Use Policy.
- An agreed policy is in place (Appendix 12: Staff/Volunteer Acceptable Use Policy Agreement, page 58, item 10) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place regarding the use of removable media by users on school devices. (see Appendix 3: Guidance for Storage and Transfer of Data, page 45)
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans etc.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

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

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The "master/administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users and replacement passwords for existing users will be allocated by the Computing and E-Safety Coordinator, or the Network Manager. Any changes carried out must be notified to the manager of the password security policy (above).
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Requests for password changes should be authenticated by the Computing and E-Safety Coordinator or Network Manager, to ensure that the new password can only be passed to the genuine user.

Staff passwords

- Passwords should be a minimum of 8 characters long and must include at least one each of – uppercase characters, lowercase characters, numbers, and special characters (e.g. £,*, #)
- The password must not include proper names or any other personal information about the user that might be known by others
- 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)
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised

Pupil passwords

- All users (at Y3 and above) will be provided with a username and password by the Computing and E-Safety Coordinator who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security and pupils in KS2 will be partly responsible for generating their own strong password.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training/Awareness

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

- at induction
- through the school's E-Safety policy and password security policy
- through the Acceptable Use Agreement

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

- in lessons through the school's E-Safety Curriculum
- through the Acceptable Use Agreement

Audit/Monitoring/Reporting/Review

The responsible person (Computing and E-Safety Coordinator) will ensure that full records are kept of:

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

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, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for E-Safety and acceptable use. It is 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 management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to and authorised by a second responsible person (the Head Teacher) prior to changes being made
- be reported to the E-Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Computing and E-Safety Coordinator 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.

Policy Statements

Internet access is filtered for all users. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will need to be considered by the Network Manager and/or Computing and E-Safety Coordinator. Staff must note that requests will not be actioned immediately as they will require the involvement of a third party organisation. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the school's E-Safety curriculum. 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:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through E-Safety awareness sessions, newsletter, VLE 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 as indicated in the School E-Safety Policy and the Acceptable Use Agreement.

Audit/Reporting

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

- the Head Teacher
- E-Safety Committee
- E-Safety Governor/Governors committee
- External Filtering provider/Academy Trust/Police on request

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

Personal Data Handling Policy

Introduction

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

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office, for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Policy Statements

- The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the *Appendix 11*: Privacy Notice and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is the Office Manager. This person will keep up to date with current legislation and guidance and will:

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

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil/student information/staff information/assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

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

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

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

Information to Parents/Carers – the Privacy Notice

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, Academy Trust, DfE, etc.) to whom it may be passed.

This privacy notice will be passed to parents/carers at the start of every academic year (or for new pupils upon enrolment) and will be available through the following channels:

- On display in the school foyer
- A paper copy on request from the school office
- Electronic copies on the school VLE and website

(See Appendix 11: Privacy Notice page 57)

Training & awareness

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

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

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences) and
- Prioritising the risks.

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

- The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

- All documents (paper or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

- Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

- Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

- All users will use strong passwords which must be changed regularly (see technical security policy). User passwords must never be shared.

- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

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

- Personal data can only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

- Personal data must not be stored on USB sticks or any other removable media as they are vulnerable to loss, damage and theft and do not offer data encryption, password protection and virus/malware protection.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.
- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data. Personal data relating to members of the school is not to be held on Dropbox or Google accounts as these are not bound by the legislation of the Data Protection Act. The school uses Microsoft's Office 365 environment for email and file sharing. Users require a user name and password to access any data and data is bound by the DPA.
- As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
- All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.
- The school recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

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

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission. The media must be encrypted and password protected and must be transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should have secure remote access to the management information system or learning platform;

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (NB. to carry encrypted material is illegal in some countries)

Staff should refer to Appendix 3: Guidance for Storage and Transfer of Data, page 45. This guidance has been put in place in order to minimise loss and damage to files and to protect personal data.

Disposal of data

- The school will comply with the requirements for the safe destruction of personal data when it is no longer required.
- The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.
- A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging/Reporting/Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals. The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example. This will be carried out by the Network Manager.

Protective Marking

The following provides a useful guide:

	The information	**The technology**	**Notes on Protect Markings (Impact Level)**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil/student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Moor Green Primary Academy

E-Safety Policy Appendices

Moor Green Primary School E-Safety Policy

Appendix 1: Glossary of terms

Pages: 5

Appendices

Appendix 1: Glossary of terms

AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from abuse, providers of the Think U Know programmes.)
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE
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
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System

NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – 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-Safety 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

Appendix 2: Legislation

It is important to note the legislative framework under which this E-Safety Policy has been produced. 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 anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website

Appendix 3: Guidance for Storage and Transfer of Data

This is not an exhaustive list but is intended to cover most of the types of documents and data created and shared by staff, and currently covers all media used. Staff should note as technologies can change, guidance regarding their use is subject to change. If staff are in any doubt regarding the secure storage and transfer of data, please consult the Computing and ESafety Co-ordinator.	Own work area on server	Staff Common drive on server [11]	Shared drive on server[12]	One Drive (personal)	One Drive (shared)[13]	School Email	Personal email (e.g. Yahoo, Gmail)[14]	Memory stick/memory card[15]	Portable device e.g. LearnPad, iPad
Planning [16]	✓	✓	×	✓	✓	✓	✓	✓	×
Resources for pupils	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEPs/IBPs	✓	×	×	✓	✓	✓	×	×	×
Pupil records and assessment data	✓	×	×	✓	✓	✓	×	×	×
Photos/videos of pupils[17]	✓	✓	×	×	×	×	×	×	×
Timetables	✓	✓	✓	✓	✓	✓	✓	✓	✓
Class/group lists, seating plans etc.	✓	✓	×	✓	✓	✓	×	×	×
Letters to parents	✓	×	×	✓	✓	✓	×	×	×
Records for CPD/ Performance Management	✓	×	×	✓	✓	✓	×	×	×
Reports	✓	×	×	✓	✓	✓	×	×	×

[11] Do not fill up the server unnecessarily. Consider using OneDrive and/or Staff documents on the Staff Portal for sharing files rather than Staff Common.

[12] All pupils have access to the Shared drive. For this reason do not save personal data here.

[13] When sharing files containing pupil data, share with the fewest people necessary, on a 'need to know' basis.

[14] Do not use personal email for transferring personal data. Personal email addresses should only be used as a last resort, for example if the school email service is not working.

[15] Most memory sticks are not encrypted and offer no virus protection. They are also vulnerable to loss, theft and damage. They are not recommended, and MUST NOT be used for files containing personal information such as reports, IEPs etc.

[16] Do not use pupils' full names in planning documents; use first names only or initials.

[17] Photos of pupils must be uploaded to the server as soon as possible and deleted from the camera's memory card. Do not save photos with pupils' names. Photos should not be emailed as this creates the possibility of them being used outside school.

Appendix 4: E-Safety Committee Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding E-Safety including monitoring the E-Safety policy and the impact of initiatives and reporting to the Governing Body.

2. Membership

2.1 The E-Safety committee will seek to include representation from all stakeholders. The composition of the group should include

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinator
- Governor
- Parent/Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- Student/pupil representation – for advice and feedback. Pupils would only be expected to take part in committee meetings where deemed relevant.

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.
2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:
Scheduling meetings and notifying committee members;

- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of meetings

Meetings shall be held once a term for a period of 1 hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the E-Safety Coordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of E-Safety
- To (at least) annually review and develop the E-Safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the E-Safety policy
- To monitor the log of reported E-Safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of E-Safety. This could be carried out through
    - Staff meetings
    - Student/pupil forums (for advice and feedback)
    - Governors meetings
    - Surveys/questionnaires for pupils, parents/carers and staff
    - Parents evenings
    - Website/VLE/Newsletters
    - E-safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Moor Green Primary Academy have been agreed
Signed by (SLT):

Date: Date for review:

Acknowledgement: This terms of reference document is based on one provided to schools by Somerset County Council

Appendix 5: Training Needs Audit

Training Needs Audit Log
Group ..... Date .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

Appendix 6: Links to Other Organisations

General Esafety Resources

Safer Internet Centre -	http://www.saferinternet.org.uk/
South West Grid for Learning	http://www.swgfl.org.uk/Staying-Safe
Childnet	http://www.childnet-int.org
Internet Watch Foundation	https://www.iwf.org.uk/
Professionals Online Safety Helpline	http://www.saferinternet.org.uk/about/helpline
CEOP	http://ceop.police.uk/
ThinkUKnow	http://www.thinkuknow.co.uk/
Netsmartz	http://www.netsmartz.org/index.aspx

UK Council for Child Internet Safety

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Cyberbullying

Digizen Cyberbullying Guidance	http://digizen.org/downloads/cyberbullyingOverview.pd
Anti-Bullying Network	http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org	http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking http://digizen.org/socialnetworking/

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

http://360safe.org.uk/Files/Documents/facebook-6

Connectsafely Parents Guide to Facebook

http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html

Facebook Guide for Educators

http://www.360safe.org.uk/Files/Documents/Facebook-Guide-for-Educators.aspx

Professional Standards/Staff Training

DfE -Safer Working Practice for Adults who Work with Children and Young People
http://360safe.org.uk/Files/Documents/Extracts-from-Guidance-for-Safer-Working-Practice-

Kent: Safer Practice with Technology
http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/ESafety/SaferPracticeWithTechnology-260509.pdf

Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs
http://360safe.org.uk/Files/Documents/ChildnetSNSleaflet(3)

Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
http://360safe.org.uk/Files/Documents/Childnettechnologyleaflet(4)

UK Safer Internet Centre Professionals Online Safety Helpline
http://www.saferinternet.org.uk/about/helpline

Working with parents and carers

Internet Matters is a website set up by the 4 major internet providers and contains lots of useful information from experts in internet safety.
http://www.internetmatters.org/

Virgin Media Switched On Families
http://keepup.virginmedia.com/switchedonfamilies

EE: Keeping children safe online -contains useful videos and links to a PDF booklet
http://ee.co.uk/ee-and-me/family-home/keeping-children-safe-online

Vodafone Digital Parents Magazine
http://www.vodafone.com/content/parents.html

Childnet Webpages for Parents & Carers
http://www.childnet.com/parents-and-carers

Get Safe Online - resources for parents
http://www.getsafeonline.org/safeguarding-children/

The Digital Universe of Your Children - animated videos for parents (Insafe)
An informative short video and links to useful fact sheets
http://www.saferinternet.org/digitaluniverse

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Lots of useful information parents of all children.
http://www.360safe.org.uk/Files/Documents/Learning-Disabilities,-Autism-and-Internet-Safety.aspx

Appendix 7: EYFS/KS1 Pupil Acceptable Use Agreement

This is how we stay safe when we use the computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (pupil):.....

Date: .....

Appendix 8: KS2 Pupil Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

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

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

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure
- I will not share it, nor will I try to use any other person's username and password.
- I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones /tablets/ USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

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

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

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

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

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

Student/Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, which it is attached.

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

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, MG Connect, website etc.

Name of Pupil	
Class	
Signed	
Date	

Appendix 9: Parent/Carer Acceptable Use Agreement and Internet permission

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school 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 online behaviour.
- The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Copies of the Pupil Acceptable Use Policies for KS1 and KS2 are attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Pupil's Name: _____ Class _____

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

- My son/daughter has signed an Acceptable Use Agreement and will receive E-Safety education in school to help them understand the importance of safe use of technology and the internet – 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 are safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

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

Signed _____ Date _____

Appendix 10: Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

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

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Parents/carers are requested to complete the permission form below.

Digital/Video Images Permission Form

Parent/Carers Name	
Pupil's Name:	Class

As the parent/carer of the above named 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. (**Please indicate yes or no.**)

YES/ NO

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

Signed	
Date	

Appendix 11: Privacy Notice

for
Pupils in Schools, Alternative Provision and Pupil Referral Units
and Children in Early Years Settings

Privacy Notice - Data Protection Act 1998

We Moor Green Primary Academy are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use of the Local Authority and the Academy Trust.

If you want to see a copy of the information about you that we hold and/or share, please contact the school's Office Manager.

If you require more information about how the DfE store and use your information, then please go to the following website:

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites the DfE can send you a copy of this information. Please contact the DfE as follows:

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street,
London SW1P 3BT
Website: www.education.gov.uk email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Appendix 12: Staff/Volunteer Acceptable Use Policy Agreement

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the 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, mobile devices, email, VLE) out of school, and to the transfer of personal data (digital or paper based) 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (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 (see section on Social Media in E-Safety Policy.)
- I will only communicate with pupils and parents/carers using official school systems. (e.g. phone, email, VLE, blogs.) Any such communication will be professional in tone and manner. I will only use a mobile phone where it is not possible to contact parents via the school – e.g. during an evening or residential educational activity. This eventuality will be planned for in the Risk Assessment for the visit. In such an event I will withhold my phone number before calling, in order to protect my privacy.
- I will not engage in any online activity that may compromise my professional responsibilities.

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 necessary I will cite my sources clearly on any documents or media I produce.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- If I am unsure of an issue regarding Copyright or Intellectual Property, I will consult the Network Manager and/or Computing and E-Safety Coordinator before downloading, distributing or publishing.

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

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without the express permission of the Network Manager and/or Computing and E-Safety Coordinator.
- 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 (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- 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.

I understand that I am responsible for my actions in and out of the 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 off the premises and my use of personal equipment on the premises 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 include a warning, a suspension, referral to Governors and/or the Academy Trust 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	

Appendix 13: Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

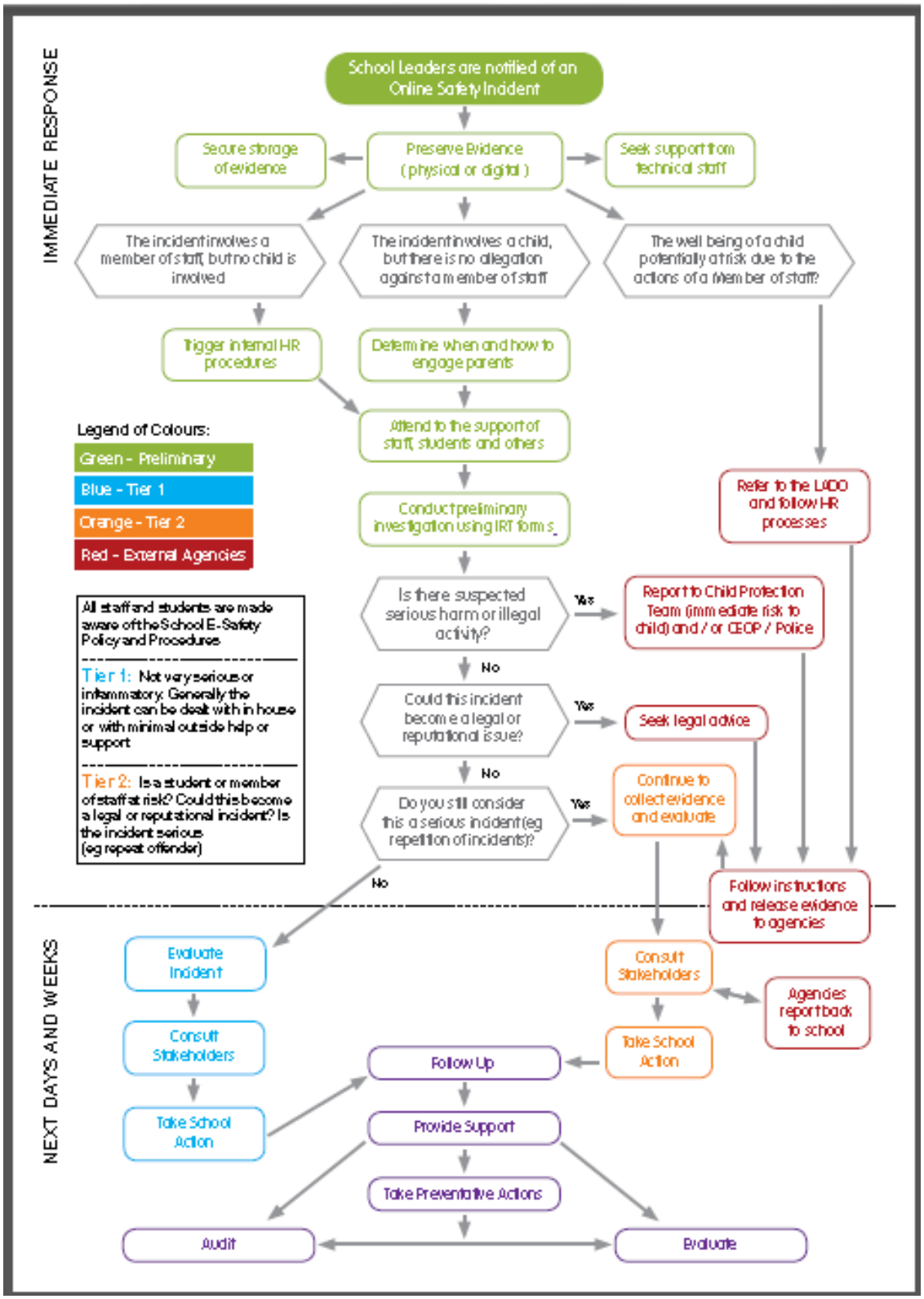
1. I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school
2. I understand that my use of school) systems and devices and digital communications will be monitored
3. I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
4. 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.
5. I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
6. I will not access, copy, remove or otherwise alter any other user's files, without permission.
7. I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
8. I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
9. I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
10. I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
11. I will not disable or cause any damage to school equipment, or the equipment belonging to others.
12. I will immediately report any damage or faults involving equipment or software, however this may have happened.
13. I will ensure that I have permission to use the original work of others in my own work

14. Where work is protected by copyright, I will not download or distribute copies (including music and videos).
15. I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices
16. 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.

Name

Signed Date

Appendix 14: Responding to Incidents of Misuse: Flow Chart (from SWGFL's Incident Response Tool)



Appendix 15: E-Safety Incident Reporting Log

Notes: To be used by staff to report ALL E-Safety Incidents. Logs can be hand written or typed using the electronic templates available on Staff Common and the Staff Portal. Log sheets must be signed and filed in the E-Safety folder in the staffroom, and the E-Safety Coordinator and/or Headteacher must be notified ASAP after the incident. Further documents from the IRT may need to be completed following the initial report.

Date	
Time	
Location of incident If in school: give room name and computer ID if known. If outside school, provide brief details e.g. '[initials]'s home address.'	
Incident details:	
Action taken: What	
By whom	
Incident reported by	
Signature	

Appendix 16: Record of reviewing devices/internet sites (responding to incidents of misuse)

Notes: To be used in the event of misuse of the school system by a pupil or member of staff, e.g. attempt to bypass filters, using inappropriate sites, or in the event of an inappropriate site bypassing the filtering system via everyday use.

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address/device	**Reason for concern**

Conclusion and Action proposed or taken

Appendix 17: Links with Other School Policies

Anti-Bullying Policy:

Page 1 Paragraph 2: Reference to cyberbullying

> ***Cyberbullying*** *- bullying via mobile phone or online (e.g. e-mail, social networks and instant messenger)*

Child Protection Policy:

Page 10 Paragraph 9.2: The Curriculum

> *9.2 Relevant issues will be addressed through the PSHE curriculum. For example, self-esteem, emotional literacy, assertiveness, power, sex and relationship education,* ***e-safety*** *and bullying.*

Appendix One, Definitions and Indicators of Abuse:

> One indicator of sexual exploitation:
> *Being groomed or abused via the Internet and mobile technology*

Data Protection Policy:

> *All sections*