Monkspath

Junior & Infant School

E-safety policy

Monkspath School will ensure that:

- Staff training needs are audited and met regularly
- We work closely with families to support them in ensuring their children use technologies safely and responsibly
- We seek the views of our families and stakeholders to inform our e-safety strategies
- We help children to know how to manage risk; to bridge the gap between school systems and less tightly manages systems at home.
- We provided a comprehensive and age appropriate e- safety curriculum that builds on children's pre- knowledge and prepares them to be safe and responsible users of rapidly changing technologies.
- We will systematically review and develop our e-safety procedures and training to ensure we provide a positive impact on our pupil's knowledge and understanding.

Document Information	
Filename	Monkspath Junior and Infant School E-Safety Policy
Date	14.04.15
Contact name	Dawn Walton
Email	S62dwalton@monkspath.solihull.sch.uk
Notes	Draft to go to whole school community May 2015

Development, monitoring, and review of this policy

This e-safety policy has been developed by:

- Digital leaders team – 2 children from each year group Years 1 – 6
- The whole school E-safety staff team including teaching/non teaching staff, all groups of adults working in school including office staff etc, our E-safety governor
- The senior leadership team
- Governors
- School council
- Parents/carers

Consultation with the whole school community has taken place through a range of formal and informal meetings

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body on	(summer 15)
The implementation of this e-safety policy will be monitored by the	Dawn Walton – E-safety lead Assistant Head Teacher Whole school – E-safety team Senior Leadership Team
Monitoring will take place at regular intervals and will take place at least	Yearly
The Governing Body will receive a report on the implementation of the e-safety policy generated by the E-safety lead *which will include anonymous details of e-safety incidents*	Termly
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be	1 year from approval date – (summer 16)

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys/questionnaires of*
- *students/pupils*
- *parents/carers*
- *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Mrs W.J. Hutchinson 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 Monkspath School, but is linked to membership of the school community. 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.

Monkspath 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.

Spiritual, moral, social and cultural development.

The development of SMSC within this policy is in line with all other policies at Monkspath School:

Spiritual

- use of imagination and creativity in their learning
- willingness to reflect on their experiences.

Moral

- ability to recognise the difference between right and wrong, readiness to apply this to their own lives.
- Understanding of the consequences of their actions

Social

- Use a range of social skills in different contexts, being able to resolve conflicts effectively.

- Interest in and understanding of the way societies and communities function

Cultural

- Willingness to participate in and respond to technological opportunities

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Monkspath School.

Governors

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors scrutinty committee, receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role within the E-safety team.

The role of the E-safety Governor will include:

- regular meetings with the E-safety Lead
- regular monitoring of e-safety incident logs, termly at full governors meetings as a minimum
- regular monitoring of filtering/change control logs

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 E-safety Lead
- The Headteacher and 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. And will seek advice from SWGFL Boost and Local Autority HR disciplinary proceedures to ensure the correct action is taken.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-safety Lead 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/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. Monitoring will take place as part of Senior Leadership meetings and appraisal. E-safety will form part of termly discussions with local authority inspectors.

The Senior Leadership Team will receive regular monitoring reports from the E-safety Lead.

E-safety Lead

The E-safety Lead will be a member of the Senior Leadership Team – Dawn Walton, Assisstant Head Teacher

- leads the e-safety teams – adult and pupil
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- Works alongside Dan Wild – Deputy Head teacher in recieving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments,
- meets regularly with the Governors Scrutiny committee - Termly
- attends relevant governors meetings
- reports regularly to Senior Leadership Team

Investigations/actions/sanctions will be the responsibility of the E-safety Lead working alongside the class teacher, year group leader and Senior Leadership Team

Network manager/technical staff

Monkspath School has a managed ICT service provided by the local authority, it is the responsibility of Monkspath School to ensure that this managed service provider carries out all the e-safety measures as suggested below

The Senior Leadership Team, Business Manager and local authority ICT service is responsible for ensuring:

- that Monkspath School's technical infrastructure is secure and is not open to misuse or malicious attack
- that Monkspath School meets required e-safety technical requirements and Local Authority E-safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which password security is maintained
- the local authority filtering policy, is applied.

- 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//remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and E-safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and support staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP)
- Visitors will sign the visitor book and indicate that they have read and understood the Staff Acceptable Use Policy Agreement (AUP). Ticking of the box in the visitor's book will indicate visitors compliance with the user agreement.
- they report any suspected misuse or problem to the Headteacher/E-safety Lead 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 policy agreement relevant to their age
- 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, tablets, 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

Child protection/safeguarding/DMS

The child protection/safeguarding/DMS 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 on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

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 Team

The e-safety team is a consultative group that has wide representation from the whole school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for termly reporting to the Governing Body.

Members of the E-safety Team will assist the E-safety Lead with:

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

Pupils

Pupils:

- are responsible for using Monkspath School's digital technology systems in accordance with the age appropriate Pupil acceptable use agreements.
- 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 tablets 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 Monkspath School's e-safety policy covers their actions out of school, if related to their membership of the school community.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Monkspath School will take every opportunity to help parents understand these issues through parents' meetings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support Monkspath 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
- their children's personal devices in school – **this is only applicable to Year 6** who bring mobile phones to school, hand them in before 9.00 am collecting them at 3.30pm, and **children who live in more than 1 home regularly**, they bring phones and belongings to school on their 'changeover days' these phones are kept securely with the other belongings during the day. <u>No other pupils may bring their personal devices to school.</u>

Policy Statements

Education – pupils

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

E-safety 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 is provided as part of computing/PHSE/other lessons and will be regularly revisited throughout the year.
- key e-safety messages will be reinforced as part of a planned programme of assemblies, e-safety focus weeks and at the start of every half termly Computing unit of work.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand (age appropriately) the need for the pupil acceptable user agreements and encouraged to adopt safe and responsible use both within and outside school]
- Staff are expected to 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 will be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (as examples, 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

Education – parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site,
- You Tube channel presentations
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community

Monkspath School will 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
- Monkspath School's website and You Tube channel presentations will provide e-safety information for the wider community

Education & Training – Staff/Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. 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 Lead will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/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 meetings/INSET days.

- The E-safety Lead 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 the Local Authority/National Governors Association /or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents
- Technology

Information

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

- Monkspath School's technical systems will be managed in ways that ensure that the school meets recommended technical requirements (outlined in Local Authority policy and guidance).
- The Business Manager and Head Teacher will carry out 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
- All users will have clearly defined access rights to school's technical systems and devices.
- All users (at Year 1 and above) will be provided with a username and secure password which are stored in the V drive where an up to date record of users and their usernames is kept. Users are responsible for the security of their username and password.
- Monkspath School uses group or class log-ons and passwords for Foundation Stage pupils and children attending holiday club who are not Monkspath pupils, but need to be aware of the associated risks
- Administrator passwords for the school ICT system, used by the Business Manager is available to the Headteacher, Deputy Headteacher and kept in the school safe. They are sealed in a signed envelope that is only to be opened when necessary
- The Business 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)

- Internet access is filtered for all users, using the local authority filter. There is a clear process in place to deal with requests for filtering changes, this is the responsibility of the Head Teacher.
- Local authority 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
- All users are expected to report any actual/potential technical incident/security breach to the Headteacher, Deputy Head Teacher or E-safety Lead.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Specific 'log ons' are in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Staff/pupils and their family members are not permitted to use school devices for personal use when being used out of school.
- Senior Leadership agreement must be sought by all staff wishing to download executable files and install programmes on school devices.
- Personal data will only be taken off site using encrypted memory sticks (provided by the school). The local authority use school email addresses. All staff will use **school email addresses only** for school communication.

Bring Your Own Device (BYOD)

- No members of the school community should use their own devices for school related activities on school premises.
- Visitors to school can use a guest log on only, this has restricted access.

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, these images may be displayed in school, parent/carer permission must be given for images to appear on the school website or be used in the press or on twitter. 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 school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or twitter, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, this will be covered as part of the acceptable use agreement signed by parents or carers at the start of the year

.

Data Protection

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

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

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. Monkspath School will ensure that they take account of relevant policies and guidance provided by local authority or other relevant bodies.

Monkspath School must ensure that:

- it 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 "Privacy Notice' and lawfully processed in accordance with the "Conditions for Processing".
- it has a Data Protection Policy - local authority
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA) – local authority
- responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) - Mrs Hutchinson (Headteacher) and Information Asset Owners (IAOs) – Sanj Dhadda (Business Manager)
- appropriate risk assessments are carried out – local authority
- It has clear and understood arrangements for the security, storage and transfer of personal data
- data subjects have rights of access and there are clear procedures for this to be obtained

- there are clear and understood policies and routines for the deletion and disposal of data
- there is a policy for reporting, logging, managing and recovering from information risk incidents – see Emergency plan
- there are clear data protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- follow the school's data protection policies
- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data, and have turned off overhead projectors.
- transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be an encrypted memory stick
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete.

Communications

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

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	🟥						YR 6 staff	🟧
Use of personal mobile phones in child areas				🟥				🟧
Use of mobile phones in social time (not in child areas)	🟥							🟧
Taking photos on personal mobile phones/cameras/tablets				🟥				🟧
Use of other personal mobile devices (as example gaming devices)				🟥				🟧
Use of personal email addresses in school for school matters.				🟥				🟧
Use of school email for personal emails				🟥				🟧
Use of messaging apps		🟥						🟨
Use of social media in personal time.		🟥						🟧
Use of blogs/Wiki's for curriculum use only		🟥					In school	
Use of mobile phones as cameras, in the role of a parent/carer, of their own child		🟥						🟧

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

- The official school email service may be regarded as safe and secure and is monitored. 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).
- Users must immediately report, (using the systems listed above for pupils and to the Senior Leadership team for adults) – in accordance with 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 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 email addresses are used in Foundation Stage, while pupils from Year 1 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as 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 Monkspath School website and only the office email address should be used to contact members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes. Monkspath School sets clear guidance for staff on how to manage risk and behaviour online.

<u>The core message is the importance of the protection of pupils, the school and the individual when publishing any material online.</u>

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012':

Personal and Professional Conduct Standard, as follows:

"A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes which set the required Standard for conduct throughout a teacher's career.

Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:

- treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position;
- having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions;
- showing tolerance of and respect of the rights of others;
- not undermining fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs;
- ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law.
- Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach, and maintain high standards in their own attendance and punctuality.

- Teachers must have an understanding of, and always act within, the statutory frameworks which set out their professional duties and responsibilities.'

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.

Monkspath School provides the following measures to ensure reasonable steps are in place to minimize 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 must 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
- Personal opinions should not be attributed to the Monkspath School or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Monkspath School's use of social media for professional purposes will be checked regularly by the Senior Leadership Team and e-safety team to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

Unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Monkspath School's and all other technical systems.

Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Monkspath 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:

Communication Technologies		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					🟥
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					🟥
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					🟥
	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					🟥
	pornography				🟥	
	promotion of any kind of discrimination				🟥	
	threatening behaviour, including promotion of physical violence or mental harm				🟥	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				🟥	

Communication Technologies	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Using school systems to run a private business				🟥	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the [school/academy]				🟥	
Infringing copyright				🟥	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				🟥	
Creating or propagating computer viruses or other harmful files				🟥	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				🟥	
On-line gaming (educational)		🟥			
On-line gaming (non-educational), except in after school and holiday club, only with supervision.				🟥	
On-line gambling				🟥	
On-line shopping/commerce – staff only.			🟥		
File sharing				🟥	

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this must referred immediately to the Head Teacher. The head teacher should refer to the SWGFL Boost advice service and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Monkspath School's 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:

If in any doubt about how to deal with the incident Senior Leaders should contact the Boost help line before taking any action – www.swgfl.org.uk/boost Password and username is securely stored with all members of the SLT.

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Report through the normal process, on the universal incident form in the 'V' drive, this will be reported to governors.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form **(except in the case of images of child sexual abuse – see below)**

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

  - Internal response or discipline procedures
  - Involvement by Local Authority or national/local organisation (as relevant).
  - Police involvement and/or action

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

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- 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 Monkspath 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.

Monkspath School actions and sanctions for children.

It is more likely that Monkspath 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:

All incidents must be reported to the DMS/Deputy Headteacher verbally immediately and then using the universal incident reporting form available in the V drive.

Communication Technologies	**Actions/Sanctions**										
	Warning	Complete incident form send to Deputy Head teacher	Further sanction |(Missed break times/cause for concern book)	Inform parents/carers	Refer to technical support staff for action re filtering/security etc.	Refer to class teacher/Year group leader	Refer to Assistant Head Teacher	Refer to Headteacher	Refer to Police - Headteachers decision	Refer to Social services/R.A.T - through DMS	Refer to PREVENT – Headteacher's decision
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		🟥					🟥	🟥	🟥 Adult	🟥 Child	🟥 Adult/child
Unauthorised use of non-educational sites during pupil contact time.	🟥	🟥				🟥	🟥				
Unauthorised use of mobile phone/digital camera/other mobile device	🟥	🟥	🟥	🟥			🟥				
Unauthorised use of social media/ messaging apps/personal email	🟥	🟥	🟥	🟥			🟥				
Unauthorised downloading or uploading of files	🟥	🟥	🟥	🟥			🟥				
Allowing others to access Monkspath School network by sharing username and passwords		🟥	🟥	🟥				🟥			
Attempting to access or accessing the network, using another pupil's account		🟥	🟥	🟥				🟥			
Attempting to access or accessing the Monkspath School network, using the		🟥	🟥	🟥				🟥			

Communication Technologies	Actions/Sanctions										
	Warning	Complete incident form send to Deputy Head teacher	Further sanction | (Missed break times/cause for concern book)	Inform parents/carers	Refer to technical support staff for action re filtering/security etc.	Refer to class teacher/Year group leader	Refer to Assistant Head Teacher	Refer to Headteacher	Refer to Police - Headteachers decision	Refer to Social services/R.A.T - through DMS	Refer to PREVENT – Headteacher's decision
account of a member of staff		🟥	🟥	🟥				🟥			
Corrupting or destroying the data of other users		🟥	🟥	🟥				🟥			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		🟥	🟥	🟥					🟥		
Continued infringements of the above, following previous warnings or sanctions		🟥		🟥					🟥		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		🟥		🟥				🟥			
Using proxy sites or other means to subvert the school's filtering system		🟥		🟥				🟥			
Accidentally accessing offensive or pornographic material and failing to report the incident		🟥		🟥				🟥			
Deliberately accessing or trying to access offensive or pornographic material		🟥		🟥				🟥	🟥	🟥	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		🟥		🟥				🟥			

Change control

This policy is subject to change control. Major revisions are listed here.

Version	Date	Owner	Comments
1	14.04.15	D Walton	Final draft of new policy
2	23.04.15	D Walton	Draft after consultation with SLT
3	20.05.15	D Walton	Final policy with user agreements to all staff and published on school website Staff user agreements to all staff to be signed and returned to the office to be filed Staff user agreement to be at front desk for all visitors to read and tick appropriate column in visitors book

Monkspath Junior and Infant School Staff (and 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 schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use in line with Monkspath School's E-Safety policy.
- That Monkspath School's 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.

Monkspath School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students/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 Monkspath 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 (eg laptops, email, learning environment etc) 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. (Please refer to Monkspath School's E-Safety Policy)
- 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 a member of the Senior Leadership Team.

I will be professional in my communications and actions when using Monkspath School's 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, this permission will only be given by either the Head Teacher or Deputy Head Teacher in exceptional circumstances. Where these images are published (e.g. on the school website) permission must be sought from parents/carers
- I will not use chat and social networking sites on school equipment in accordance with the school's policies. Monkspath School's Twitter account can be accessed only by designated members of staff
- I will only communicate with pupils using my internal email address and parents/carers using the school office email address, answers to parents/carers emails should be forwarded on by the school office. Any such communication will be professional in tone and manner. Staff should not use their own email addresses/mobile phones/social networking accounts to communicate with either pupils or parents/carers.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Monkspath School:

- I will not use my own devices except my mobile phone in school. I will follow the rules set out in this agreement and the E-Safety/Child Protection policy)
- I will not use my mobile phone in any public area of the school or when I am with the pupils.

- 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 from the Senior Leadership Team) 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 seeking permission form the Senior Leadership Team.
- 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 Local Authority Personal Data 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.

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

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

I understand that I am responsible for my actions in and out of Monkspath 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 Monkspath School

- I understand that if I fail to comply with this acceptable use policy, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to governors and/or the local authority and in the event of illegal activities the involvement of the police. (see E-Safety Policy)

I have read and understand the above and agree to use Monkspath School's 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. This agreement is in relation to both this acceptable use policy and the asset policy (attached).

Staff/Volunteer Name

Signed

Date

Acceptable use policy agreement for Foundation Stage and Year 1.

This is how we stay safe when we use computers:

- I can use the computers if it is planned for me.
- I will only use activities that a teacher or another grown up who works at school has let me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or another grown up who works at school, if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or another grown up who works at school, if I see something that upsets me on the computer.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child

Acceptable use policy agreement for Years 2, 3 and 4

This is how we stay safe when we use computers:

- I will only use the computers or tablets if I know I have permission from an adult at school.
- I will only use suitable programmes and websites that a teacher or another grown up who works at school lets me use.
- I will take care of the computer and other equipment and tell an adult if I find any problems.
- I will ask for help from a teacher or another grown up who works at school, if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or another grown up who works at school, if I see something that upsets me on the computer or an unfamiliar pop up.
- I will not share any personal information online.
- I will be polite, respectful and responsible towards others online, I will not cyberbully.
- I will take care to check that information I find online is accurate and I can trust it.
- I know that if I break the rules I might not be allowed to use a computer, and that an adult may investigate any inappropriate use of technology that affects me or my friends in our school community

Signed (child

Acceptable use agreement for Years 5 and 6.

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 school's ICT systems and other users.

For my own personal safety:

- I understand that Monkspath 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 on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details and photographs)
- I will not meet with anyone that I have communicated with on-line, if someone asks me to meet them I will tell an adult I trust.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. I know I can speak to an adult I trust, use the CEOP button or Whisper button on our school website or our worry boxes.

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

- I understand that the Monkspath School's systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try 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 Monkspath School's systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (eg YouTube),
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. I will not cyberbully at school or at home.
- 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 Monkspath School:

- I will not use my own personal devices (mobile phones/USB devices) in school.
- 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 these 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 not use social media sites of any kind on any school device.

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 Monkspath School has the right to investigate reports and 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 our school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include; loss of access to the school network/internet, contacting parents/carers 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 ICT systems.

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

- I use Monkspath School's systems and devices (both in and out of school)

- I use my own equipment outside of Monkspath School in a way that is related to me being a member of our school community eg. communicating with other members of the school, accessing school email, website etc.

Name of Pupil

Class

Signed

Date

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Monkspath School's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

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

I know that my son/daughter has signed an Acceptable Use Agreement and has will receive, e-safety education 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 will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

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

Signed

Date

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students/pupils and members of staff may use digital cameras/iPads 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, in line with our home school agreement and in some cases for the protection of individuals, parents/carers will never publish photos/ images/ videos of school life on social media on open forums. They agree to keep all publications to closed friendship groups, and will never make any derogatory comments about pupils at the school on any social media.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children to be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

Digital/Video Images Permission Form

Parent/Carers Name

Student/Pupil Name

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

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

Signed

Date

The school uses Google Apps for Education for pupils and staff.

The following services are available to each pupil/student and hosted by Google as part of the school's online presence in Google Apps for Education:

Pupils collaboratively create, edit and share files and websites for school related projects. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent/Carers Name

Student/Pupil Name

As the parent/carer of the above student/pupil, I agree to my child using the school using Google Apps for Education.

Signed

Date