MONKSDOWN Primary School

Online Safety Policy

Spring 2020

Scope of the Policy

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

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

1. Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

2. Roles and Responsibilities

Governors:
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (Jane Moores). The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee / meeting

Headteacher / Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included section 7h – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their online 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 online 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 MGL Technician.
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

Online Safety Coordinator:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

The Network Manager, Technical Staff and Computing Coordinator are 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 online safety technical requirements and any Local Authority Online Safety Guidance.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- that the use of the network and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Online Safety Coordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

- they have an up to date awareness of online safety matters and of the current *school* Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/ Safeguarding Lead/ Online Safety Coordinator.
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Officer

Should be trained in Online 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

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.

- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online 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 / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online 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 the school

5. Policy Statements

Whilst the PIES (policies, infrastructure, education and standards) model forms the basis of the school's approach to Online Safety the school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

As part of the Online Safety policy the school will also manage:

- Education
- Technical – infrastructure / equipment, filtering and monitoring
- The use of digital images and video
- Data protection
- Digital communications
- Unsuitable/inappropriate activities
- Incidents of misuse

a) Education (see Computing Policy)

b) Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety 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
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by Mrs Smith who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- The "administrator" passwords for the school ICT system, used by the Network Manager (MGL Technician) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- Internet access is filtered for all users. Illegal content, potentially harmful including that of terrorist or extremist nature is filtered by our broadband provider or our 'Smoothwall' system.
- *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.* (
- Appropriate security measures are in place to protect all equipment from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- An agreed policy is in place (AUP – see Appendices) for teachers/pupils and visitors.

c) Mobile Technologies

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

d) The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and do so only with the appropriate permissions.

6. Data Security and Protection

Staff must ensure that all data is handled as per our policies. 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.

7. Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies, the school ensures the following good practice:

- The official school email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at Key Stage 1, while pupils at Key Stage 2 will be provided with individual school email addresses for educational use when appropriate and necessary.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

8. Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

9. Responding to incidents of misuse

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

In the event of an Online Safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the following incident flowchart. All incidents will be recorded and reported to the relevant parties and organisations.