

# Online Safety Policy

## Penkridge Middle School

Updated Jan 2017

## Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

### 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 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*.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

### Headteacher and Senior Leaders:

- The Headteacher is responsible 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 Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online 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 Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. **Mr L Meredith Online Safety Coordinator** and **Mr R West Safeguarding lead** will take responsibility for the day to day monitoring of Online Safety incidents.
- The Headteacher and another member of the Senior Leadership Team 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 in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

## **Online Safety Coordinator: (Mr L Meredith - PMS Online Safety Coordinator)**

### **The Online Safety Co-ordinator will/is responsible for:**

- leads the Online Safety committee
- 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
- liaises with school ICT technical staff
- Generates reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering control logs
- attends relevant meeting of governors Health, Safety and Premises committee
- reports regularly to Senior Leadership Team
- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression

## **Network Manager / Technical staff:**

ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.

RM provides Penkridge Middle School with the filtering solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied. Schools are able to control their own permissions and add/amend to the defaults. The Penk Valley helpdesk can be contacted if schools require assistance with this.

ICT Technician is responsible for ensuring:

- the school's filtering policy as related to the above system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see Filtering Policy)
- that he / she keeps 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, Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Co-ordinator for investigation, action and if appropriate sanctions.
- that monitoring software and 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 Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Co-ordinator for investigation, action and if appropriate sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- pupils understand and follow the school Online Safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of Online Safety issues related to the use of mobile phones and cameras and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Child Protection Officer (R. West and if absent N. Frost or S. Hodson)

should be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal or inappropriate materials;
- inappropriate on-line contact with adults and strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

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

## Online Safety Committee

Members of the Online Safety committee (or other relevant group) will assist the Online Safety Coordinator with:

- the production, review and monitoring of the school Online Safety policy documents.
- the production, review and monitoring of the school filtering policy

## **Pupils:**

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, and digital cameras. They should also know and understand school policies on the taking use of images and on cyber-bullying.
- 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local Online Safety campaigns / literature*. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

## **Scope of the Policy**

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) 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 to such extent as is reasonable, to regulate the behaviour of students 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 Online 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.

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 out of school.

## **Education – Students / Pupils**

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

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

A planned online safety curriculum should be provided as part of Computing and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school / academy.
- 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 students 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 students are allowed to freely search the internet, staff should 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 (eg 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 online 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, Learning Platform
- Parents / Carers Online Safety evenings
- High profile events e.g. Safer Internet Day
- Reference to the relevant web sites / publications