Unlocking the Magic of Learning

Whoberley Hall

Primary School

E Safety Policy

Date: October 2017

Date to be reviewed: October 2018

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. 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 (see appendix for template policy).

The school will deal with such incidents within this policy and associated behaviour and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Governors

Governors are responsible for reviewing the effectiveness of the policy in conjunction with the regular safeguarding policy. This will be carried out by the Governors receiving information about any breaches of this policy. The Safeguarding Governor will assume the role of monitoring such breaches and any other issues regarding online safety. This should include discussing online safety at termly safeguarding meetings.

Headteacher

- 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 Safeguarding Lead.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of an online safety allegation being made against a member of staff.

- The Headteacher is responsible for ensuring that the Safeguarding Lead 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 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 monitoring reports from the Safeguard Lead.

Teaching and Learning

The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught how to evaluate Internet content. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Online Safety Lead (Safeguarding Lead)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- 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 technical staff
- Receives reports of online safety incidents and informs the headteacher
- Meets termly with Safeguarding Governor to discuss current issues, review incident logs and filtering control logs
- Attends relevant meeting of Governors
- Reports regularly to Senior Leadership Team

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 report any suspected misuse or problem to the Headteacher ,or Safeguarding lead.
- All digital communications with pupils, parents and 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

- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

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 and 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* and on-line pupil records
- Usage of images and videos posted to Class Dojo
- Their children's personal devices in the school on Toy Days.

Designated Safeguarding Lead

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

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
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good 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
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Coventry Local Authority can accept liability for the material accessed, or any consequences of Internet access. (see managing internet access for further details)

- Introducing the eSafety Policy to pupils Surf Safe rules will be posted in all classrooms rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Policy Statements

Education – Pupils

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 pastoral activities
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils 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.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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, Class Dojo
- Parents evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites e.g. swgfl.org.uk www.saferinternet.org.uk/

Education & Training – Staff / Volunteers

It is essential that all staff understand their responsibilities, as outlined in this policy.

This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.

The Online Safety Coordinator will provide advice guidance to individuals as required.

Managing Internet Access (both pupils and staff)

Information system security, School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly.

Access to Laptops/I-Pads

- Children from Year 2 to Year 6 will have access to laptops and their own personal login. This will enable children to manage their work on their own personal account. It will also enable staff to monitor children's usage of Internet closely through their accounts. Children in KS2 all have personalised passwords and must login as themselves. The children also have access to I-pads. The laptops have monitoring software recommended by the LEA.

- Reception, Nursery and Year 1 children have access to I pads to meet their ICT development needs. These are carefully restricted to ensure children don't access inappropriate material and the children are carefully monitored by staff with the Early Years setting.

E-mail

Pupils may only use their school generated office 365 email accounts in school. Pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils will not be able to do the following, because our email is a closed system: reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the Website. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

The school will block access to social networking sites. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Primary pupils are not old enough to legally access social network spaces, therefore no member of staff should be friends with a pupil on any social network space, as it causes a safeguarding risk. In addition it is highly advisable that staff are not friends with parents of the school, as this may lead to their professionalism being called into question.

If staff do use social media, it is essential that their security settings are set at the highest possible setting and that only people who are their personal friends can access their content.

Managing filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. The school currently uses the LA approved filter, which can only be modified by the Headteacher, Deputy Head and ICT coordinator. If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, Safeguard Lead or Headteacher. Steps can then be taken to ensure the website is blocked and no longer accessible in school. Filtering for teachers and children is different to enable to use website such as YouTube for educational purposes, whilst ensuring children can't access inappropriate content. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press. (This is covered by the image consent form)

- In accordance with guidance from the Information Commissioner's Office, parents 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 on social networking sites, nor should parents comment on any activities involving other pupils in the digital images.

- Staff and volunteers are allowed to take digital images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

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

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs without parental permission

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material. Pupils should not normally bring mobile phones to school. When this is absolutely necessary, pupils' mobile phones will be given to teaching staff at morning registration and returned to pupils at the end of the school day. The sending of abusive or inappropriate text messages, I-messaging or any other instant messaging service is forbidden. The use of video messaging services such as Face time, Skype and any other social media video messaging is also forbidden unless being used for an academic purpose and is approved by the Head Teacher. Staff will use a school phone where contact with pupils is required. Staff should not use personal mobile phones during designated teaching sessions.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (also see the schools Data Protection Policy) 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.

Staff must ensure that they:

- 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system,

- The device must be password protected
- 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

When personal data is stored on a memory, portal hard drive or any portable storage solution,

- The data must be encrypted and password protected
- The data must be securely deleted from the device, once it has been transferred or its use is complete

Social Media - Protecting Professional Identity

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to students / 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 school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established (ie PTA) there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse

- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites
-

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Other Incidents

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

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

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

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

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

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

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

    - Internal response or discipline procedures

    - Involvement by Local Authority

    - 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
    - Adults material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Other criminal conduct, activity or materials

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator. This policy is the Governors' responsibility and they review its effectiveness regularly. They do this during reviews conducted between the, Designated Child Protection Coordinator & the Governor with the responsibility for Child Protection. Ongoing incidents would be reported to the full governing body.