e-Safety Policy

Safeguarding pupils, staff and school in a digital world

September 2015

Table of Contents

Introduction

This e-Safety policy recognises our commitment to e-safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the 'Every Child Matters' agenda.

We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to e-Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

Nb. *for the purposes of clarity and consistency throughout this document the person in school who is taking a lead on e-Safety is called the e-Safety manager.*

The person in school taking on the role of e-Safety manager is Miss Sarah Harvey

This e-Safety policy was created by the Senior Management Team.

The policy was reviewed: September 2015

The policy is due for review no later than: September 2016

Responsibilities of the School Community

We believe that e-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Senior Management Team accepts the following responsibilities:

- *Identify a person (the e-Safety manager) to take responsibility for e-Safety and support them in their work.*
- *Ensure adequate technical support is in place to maintain a secure ICT system.*
- *Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets*
- *Ensure liaison with the Governors*
- *Develop and promote an e-Safety culture within the school community*
- *Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have e-Safety included as part of their induction procedures*
- *Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to e-Safety*
- *Receive and regularly review e-Safety incident logs; ensure that the correct procedures are followed should an e-Safety incident occur in school and review incidents to see if further action is required*
- *Take ultimate responsibility for the e-Safety of the school community*

Responsibilities of the e-Safety Manager

- Promote an awareness and commitment to e-Safety throughout the school
- Be the first point of contact in school on all e-Safety matters
- Create and maintain e-Safety policies and procedures
- Develop an understanding of current e-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in e-Safety issues
- Ensure that e-Safety education is embedded across the curriculum
- Ensure that e-Safety is promoted to parents and carers
- Liaise with the Local Authority and other relevant agencies as appropriate.
- Monitor and report on e-Safety issues to the the Leadership team and Governors as appropriate.
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable.
- Ensure an e-Safety incident log is kept up-to-date.

Responsibilities of all Staff

- Read, understand and help promote the school's e-Safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current e-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed e-Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all e-Safety incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance

- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all e-Safety incidents to appropriate members of staff
- Discuss e-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting e-Safety
- Read, understand and promote the pupil AUP with their children
- Discuss e-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's e-Safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safety awareness
- Ensure appropriate funding and resources are available for the school to implement their e-Safety strategy

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in

our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver e-Safety knowledge and understanding and ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

We believe that learning about e-Safety should be embedded across the curriculum.

We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the AUP.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and Learning Platform.

We will ask all parents to discuss the pupil's AUP with their child and return a signed copy to the school.

We request our parents to support the school in applying the e-Safety policy.

Managing and safeguarding ICT Systems

The school will ensure that access to the school ICT system is as safe and secure as reasonably possible.

All internet access in school is controlled through the local authority filtering system. (see below) A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

Forensic software is installed on all computers to monitor IT use.

Any administrator or master passwords for school ICT systems are kept secure and available to at least two members of staff, (Head Teacher and Office manager.)

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by the e-safety manager.

Only staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by Education Walsall. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. Any inappropriate material accessed or discovered on a computer should be reported to the e-safety manager or line manager.

Using the Internet

We provide the internet to

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using, the school ICT systems or a school provided laptop or device and that such activity is monitored and checked.

All users of the school ICT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Using email

Email is regarded as an essential means of communication. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

As part of the curriculum pupils are taught about safe and appropriate use of email.

Publishing content online

ie. Using the Learning Platform, blogs, wikis, podcasts, social network sites

School Learning Platform:

The school maintains editorial responsibility for the school learning platform content to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school learning platform by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the learning platform is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the learning platform and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Online material published outside the school:

Pupils use of online publishing outside of school, eg. Social networking is discouraged. However it is recognised that social networking by pupils will occur out of school and so staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of these outside school as they are in school. It is advised that staff do not set up "friendships" with pupils via social network sites.

Material published by pupils and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of staff will be considered a breach of school discipline and treated accordingly

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

Using mobile phones

We recognise that the multimedia and communication facilities provided by a mobile phone can provide beneficial opportunities for pupils. However their use in lesson time is not allowed and they are handed to a member of staff to be locked away in a secure place, until needed.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

Using other technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safety point of view.We will regularly review the e-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behavior to those outlined in this document.

Protecting school data and information

School recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their e-Safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with appropriate levels of access to the schools management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data

Dealing with e-Safety incidents

All e-Safety incidents are recorded in the School e-Safety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious e-Safety incident, concerning pupils or staff, they will inform the e-Safety manager, their line manager or head teacher who will then respond in the most appropriate manner. Instances of **cyberbullying** will be taken very seriously by the school and dealt with using the school's anti-bullying procedure. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create an information security risk, will be referred to the school's e-Safety manager, appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserve the right to monitor and search any technology equipment on the premises, including personal equipment, including when a breach of this policy is suspected.

Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly

- *Responsibility for handling serious incidents will be given to a senior member of staff*
- *Parents and the pupil will work in partnership with staff to resolve any issues arising*
- *There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies*

The following activities constitutes behavior which we would always consider unacceptable (and possibly illegal) :

- *accessing inappropriate or illegal content deliberately*
- *deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent*
- *continuing to send or post material regarded as harassment, or of a bullying nature after being warned*
- *using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)*

Appendix

Guidance for safer working practice for adults who work with children and young people (438.5Kb) DCFS 2009.