October 2015

E-Safety Policy

The Bluecoat School, Stamford

Introduction

The term e-safety is used primarily to describe proactive methods of educating and safeguarding children and young people while they use digital technology. In order for children and young people to remain safe, we should educate them not only of the dangers but also inform them who they can contact should they feel at risk and where to go for advice, while still promoting the many benefits of using digital technology, thereby empowering them with the knowledge and confidence of well-researched good practise and continuing development. (Lincolnshire Schools E-Safety Policy and Guidance 2010)

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.

It should be remembered that digital technology reaches far and wide and although most of this document refers to the use of computer technology and laptops the scope for e-safety extends to technologies such as: Ipads, Ipods, Iphones, Xbox systems, Playstation systems, Nintendo systems, mobile phones, smart phones, PDA's and anything else which allows for interactive digital communication.

We want children to be using digital technology. We believe that digital technology can be used to:

- raise educational standards and promote pupil achievement.
- develop the curriculum and make learning exciting and purposeful.
- enable pupils to access a wide span of knowledge in a way that ensures their safety and security.
- enhance and enrich their lives and understanding.

E-safety should be less about restriction and more about education about the risks as well as the benefits so that all users feel safer online. It is about developing safer online behaviours both in and out of school.

E-safety should be a focus in all areas of our curriculum and staff will reinforce e-safety messages at every opportunity. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such an 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 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. In the case of both acts, action can only be taken over issues covered by the school's published Behaviour Policy.

The Bluecoat 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.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within The Bluecoat 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 receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor within the Safeguarding governor role.

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 Co-ordinator.
- the Headteacher and (at least) another member of 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.
- the Headteacher /Senior Leaders are responsible for ensuring that the E-Safety Co-ordinator 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.
- the Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator
- a commitment to e-safety is an integral part of the safer recruitment and selection process for staff and volunteers.

E-Safety Co-ordinator:

- 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/relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

- reports regularly to the Senior Leadership Team and governors
- will ensure that the e-safety curriculum is taught in each year group and monitor coverage

Network Manager/Technical staff: (currently provided in school by ARK ICT Solutions)

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 e-safety technical requirements and any Local Authority Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy is applied and updated on a regular basis.
- 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 .
- that monitoring software/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 e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (see Appendix 2).
- they report any suspected misuse or problem to the Headteacher for investigation.
- all digital communications with pupil/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 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
- in their own use of Facebook, Twitter and other social networking sites, they must not post material (including text or images) which damage the reputation of the school or which cause concern about their or any other member of staffs suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to school via these networks.

- it is never acceptable to accept a friend request from pupils. It is inadvisable to accept friend requests from ex-pupils. It is inadvisable to accept or initiate friend requests with parents or carers.
- their passwords are kept private. Children should not be using a computer logged on to a teachers account. If this is essential there should be 1:1 supervision.

Child Protection / Safeguarding Officer:

should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues that may 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 Policy (see Appendix 3)
- 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 (they will only switch the screen off or put the device upside down on the desk, tell the adult in the room who will tell the e-safety coordinator or child protection officer. This will be logged centrally.)
- 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 e-safety practice when using digital technologies out of school and realise that the school's E-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 Bluecoat School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, joint parent and pupil workshops, the school website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Training – Staff / Volunteers

It is essential that all staff receive appropriate e-safety training and understand their responsibilities, as outlined in this policy.

Training – Governors

Governors will be invited to take part in e-safety training/awareness sessions, including those provided for parents and pupils, with particular importance for those who are members of any group involved in technology/e-safety/health and safety/child protection.

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 e-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.
- if appropriate all users (including pupils at KS2 and above) will be provided with a username and secure password by ARK ICT Solutions who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year. In KS1 class log-ons will be used.
- the "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- the School Bursar 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
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- 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.
- an agreed procedure is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. This involves the use of a temporary password to access the system.
- An Acceptable Use Policy is in place regarding the extent of personal use that users (staff/ students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An Acceptable Use Policy is in place regarding the use of removable media (eg memory sticks/ CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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 the following risks:

- 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 eg. on social networking sites.
- 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, 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/video images that students/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.
- written permission from parents or carers will be obtained before photographs of pupils are published on the school website

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.

The 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
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- 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
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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, memory stick or any other removable media:

- the data must be encrypted and password protected
- 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, in line with school policy (below) once it has been transferred or its use is complete

Communications

Mobile phones are permitted for staff in school but are restricted to the staffroom only during break times. Pupils and any other visitors including volunteers, to the school are not permitted to have mobile phones on the premises. Visitors/volunteers are advised not to bring mobile phones onto the premises. However, if they choose to do so, they will be securely stored at reception.

Staff should not use their own IPad's as these are not subject to the schools filtering system.

School email addresses are for school related business only. Staff should not use personal email addresses in school without permission from the Headteacher. Pupils may only use the class email address provided for them, which is monitored by class teachers.

Messaging apps and social media may be used as part of lessons but with the permission of the Headteacher.

Blogs are permitted on the school website only and are subject to continuous monitoring.

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. Pupils should only use the school email service to communicate with others when in school. Staff should only use the school e-mail service to conduct school business.
- users must immediately report, to the E-Safety Co-ordinator/Headteacher/Chair of Governors/LADO, 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 / group email addresses may be used at KS1, while students / pupils at KS2 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 school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Schools 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.

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.

Unsuitable / inappropriate activities

Some internet activity for example, accessing child abuse images, distributing racist material or use of the school system to enable the promotion of extremism or radicalisation is illegal and is banned from school and all other technical systems. Other activities for example, cyber-bullying are also 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.

It is expected 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.

Responding to incidents of misuse

In the event of any incident or suspected incident of misuse, the staff member should immediately complete an e-safety incident form (see appendix 1) and hand it to the Designated Safeguarding Officer (DSO) without delay. The DSO will then investigate the reported incident and take appropriate action in accordance with school safeguarding procedures.

Signed: _____Chair

_____ Headteacher

Date: _____

Last updated: October 2015

Review date: October 2018

Appendix 1

The Bluecoat School

E-safety Incident Report Form

Name(s) and role(s) of person/people involved in the incident
Date and time of concern : (please note this form should be completed immediately a concern arises)
Your account of the concern : (what was said, observed, reported and by whom)
Your response : (what did you do/say following the concern)

Your name :
Your signature :
Your position:
Location of Incident:
Date and time of this recording :
Action and response of designated safeguarding officer Name: …….. Date:……..

Appendix 2

Acceptable Use Policy – Staff

Please note: All Internet and email activity is subject to monitoring
You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only (currently blogging). Staff using social networking for personal use should never undermine the school, its staff, parents or children. It is not recommended that Staff become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including email, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student.

Data Protection – If it is necessary for you to take work home, or off site, you should not have any school related personal data on your devices without prior permission from the Headteacher.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent of the school. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment (i.e. mobile phones, iPads etc.) is not generally permitted within school or for school business, however the Headteacher may use discretion on an individual basis.

Viruses and other malware - any virus outbreaks are to be reported to ICT Support as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with pupils.

Name:

Signature: **Date:**

Appendix 3

Acceptable Use Policy – Pupils

Please note: All Internet and email use is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for, or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (Pupil):