Bishop Alexander L.E.A.D. Academy
A L.E.A.D. Academy

Bishop Alexander L.E.A.D Academy

e-safety Policy

Ratified by Governors on:

Review date: January 2016

Signed by Chair of Governors……………………………………………………………………

ICT in the 21st Century is seen an essential resource to support learning and teaching, as well as playing an essential role in the everyday day lives of children, young people and adults. Therefore at Bishop Alexander LEAD Academy we aim to build in the use of these technologies in order to give our young people with the skills to access lifelong learning and employment safely.

E-safety involves pupils, staff, governors and parents making best use of technology and information and so we want to create and maintain a safe online and ICT environment for Bishop Alexander LEAD Academy.

Bishop Alexander Primary School e-safety Policy was developed and agreed by the whole staff and has the full agreement of the Governing body. The policy was developed from the NGfL policy and government guidance. The policy was approved at a meeting of the Governing body.

Purpose

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature attitude.

Benefits

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to professional bodies and experts in many fields for pupils and staff;

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the e-safety policy and reviewing the effectiveness of the policy, regularly meeting with the e-safety coordinator and monitoring e-safety logs.

Headteacher:
The Headteacher will be responsible for ensuring safety of the school community (including e-safety) although day-to-day responsibility will be delegated to e-safety coordinator.

e-safety Coordinator:
The e-safety coordinator takes on responsibility for e-safety issues, leads the development and review of e-safety policies and documents, ensures all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place, provide training and

advice to staff, liaises with school IT Technician and receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teachers:
All teachers will be expected to model and educate pupils on how to use the internet safely, guiding pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.All teachers should be aware of the procedures to be followed in the event of a e-safety incident.

Teaching and Learning
Internet use is a statutory part of the curriculum and a necessary tool for staff and pupils, therefore the school has a duty to provide pupils with quality internet access as part of their learning experience:

- The school internet access will be tailored specifically for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for internet use and taught what use is acceptable.
- Pupils will be educated in the effective use the internet in research, including skills of knowledge location, retrieval and evaluation.
- As part of the new curriculum, all year groups have digital literacy units that focus on different elements of staying safe online, including how to use a search engine, digital footprints and cyber bullying.

Internet Content

The school Internet access will be designed expressly for pupil use and will include filtering provided by the Education Authority or a third party and be appropriate to the age of pupils. The school will work in partnership with parents, LEAD Academy, LA or third party provider, DfES and the Internet Service provider to ensure systems to protect pupils are reviewed and improved. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives regarding Internet use.

The school will where possible ensure that the use of Internet derived materials by staff and by 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.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions, applying settings to block and screen webpages 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 Nottinghamshire County Council can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

Safeguards

If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the e-safety coordinator.

Security and Passwords

Passwords are an important aspect of computer security and protection. A user who carelessly selects a password may compromise an entire network. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff should always 'lock' their computer if they are going to leave it unattended. It is good practice for passwords to be changed on a regular basis.

School Web Site

The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified. Images of individuals will not be used and names of pupils shown in any photographs will not be included. Furthermore, pupils' full names will not be used anywhere on the Web site. Written permission from parents or carers will be obtained before photographs of pupils or their work can be published on the school Web site. Children's work will only be identified by first name and/or year group. The school will keep a record of all pupils who do not have consent for use of their work or photographs on the school website. Pupils will also have individual logins and usernames for additional facilities provided on the web page e.g. blogs, news reports, which have to be authorised and approved by staff before being displayed.

Emails

Emails are a quick and preferred method of communication, ensuring beneficial and appropriate usage is very important. Pupils may only use approved email accounts on the school system and must immediately inform a teacher if they receive an offensive e-mail. Pupils must not reveal personal information relating to themselves or others in an email communication. Emails sent to external organisations should be written carefully and authorised before sending. Chain letters, advertising, spam and other unknown sources will be deleted without opening or forwarding.

Social Networking

Pupils will not be allowed access to public or unregulated social networking sites (such as, Facebook and Twitter). Children should use only regulated educational chat environments where an educational benefit has been established e.g. school blogs and all communication must be authorized by class teachers before it will be displayed. Chat room safety emphasized, ensuring personal information is not shared in any form. Pupils and parents are advised (at parent e-safety meeting and parent support documents) that social networks are not appropriate for primary aged pupils, including those on games such as the online Minecraft game. Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

Staff and particularly teachers, should not put any information onto the site that appertains to school, staff or pupils. In their own interests, staff need to be aware of the dangers of putting personal information on social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for children and their families or friends having access to staff outside the school environment.

Emerging Internet uses

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will not be allowed mobile phones during school time. Any mobile phones brought inadvertently into school should be kept in the school office during the school day. The sending of abusive or inappropriate text messages is forbidden.

Internet access

The school allows Internet access to all staff and pupils. In the Foundation Phase, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. Key stage 1 and 2 pupils will be able to access the internet for specific work and due to individual pupil logins the laptop use will be monitored closely.

Digital/Video Cameras and Photographs

Pictures, videos and sound are not directly connected to the internet but images are easily transferred. Therefore, pupils will not use digital cameras or video equipment at school unless specifically authorized by staff. Parents and Carers are only permitted to take photos/videos of their own child in school events, if they sign to say that they will not share these on social networking sites or publication of any kind, if other pupils are in the background.

Staff should always use a school camera to capture images and should not use their personal devices. Photos taken by school are subject to the Data Protection act.

Staff

All staff including teachers, supply staff, teaching assistants, support staff and administrative staff will have access to the School e-safety Policy, and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

ICT system security

The school ICT systems will be reviewed regularly with regard to security and any Academy/DfES guidance will be adopted. Only IT technicians will be able to introduce and install new programs onto the network (weekly visits to repair, maintain, update IT equipment). Virus protection is installed and updated regularly. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and Freedom of Information Act.

Reporting

All breaches of the e-safety policy need to be recorded in the e-safety reporting folder that is kept in the office. The details of the user, date and incident should be reported. Evidence and incidents must be preserved and retained.

Incidents which may lead to child protection issues need to be passed on to Mrs N. Spencelayh (Headteacher) immediately – it is their responsibility to decide on appropriate action not the class teacher.

Incidents which are not a child protection issue but may require long term intervention (e.g.cyberbullying) should be reported to Miss S. Tyers (e-safety coordinator) or Mrs N. Spencelayh (Headteacher) the same day.

Allegations that involve the staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and staff'. If necessary the LA's LADO should be informed.

The curriculum covers how pupils should report incidents and there are supporting links to websites and information on the school webpage.

Handling e-safety Complaints

Complaints of Internet misuse will be dealt with by a senior member of staff, complaints about staff misuse must be referred to Headteacher and complaints of a child protection nature shall be dealt with in accordance with school child protection procedures. Parental complaints can be carried out as any other complaint, details of which are available on school webpage.

e-safety coordinator: S. Tyers
e-safety governor:
IT technician: Lee Jepson