Landau Forte Academy Moorhead

Name of Policy: Online Safety Policy

Date of Policy: November 2015

Member of Staff responsible: M.Trimbee

Review date: January 2017

Signature: _____ Chair of Governors

Date Approved: _____

Online Safety Policy

Our Online Safety Policy has been written by the Academy, building on the Kent Online Safety Policy and government guidance. The Online Safety Policy relates to other policies including those for bullying and child protection.

TEACHING AND LEARNING

Why the Internet and digital communications are important

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. Rules for acceptable use are displayed in classrooms and other areas where the internet may be used.

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 shown how to publish and present information to a wider audience.

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 will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content e.g. using the Child Exploitation and Online Protection (CEOP) Report Abuse icon or Hector's World (Think U Know).

MANAGING INTERNET ACCESS

Maintaining information system security

Local Area Network (LAN) security issues include:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. Misuse of the network will result in disciplinary actions being taken.
- Workstations are secured against user mistakes and deliberate actions.
- The Server is located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network is installed and current, using Symantec End Point Protection and automatic updates.
- Wireless access to the Academy network is protected by a network key.

Wide Area Network (WAN) security issues include:

- All Internet connections are connected through a firewall at Landau Forte College, Derby to ensure adequate filtering and security protection are in place.
- Firewalls and switches are configured to prevent unauthorised access.
- The security of the Academy information systems will be reviewed regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal data transported on Portable media must be encrypted or password protected.
- Portable media may not be used by pupils without specific permission followed by a virus check. (Staff using portable media are encouraged to virus check their media regularly.)
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the Academy's network will be regularly checked.

The IT systems manager and IT technician will review the system capacity regularly.

E-mail

E-mail for staff is provided by the Academy.

Staff have e-mail addresses which take the form of initialsurname@lfadm.org.uk

Pupils can send or receive emails through the Learning Platform. Pupil e-mail is a walled garden as default which means they cannot e-mail people beyond the Academy. Wider access may be given for specific projects in the Academy.

Pupils may only use approved e-mail accounts. Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to external organisations should be written carefully as this is the same as sending a letter on school headed paper.

The forwarding of chain e-mail is not permitted.

Published content and the Academy website

Staff or pupil personal contact information will not generally be published. The contact details given online should be the Academy office.

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

Publishing pupils' images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consideration will be given to using group photographs rather than full-face photos of individual children.

Pupils' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.

Parents will be clearly informed of the Academy policy on image taking and publishing.

Written permission from parents or carers will be obtained before photographs of pupils are published on the Academy Web site.

Work can only be published with the permission of the pupil and parents/carers.

Pupil image file names will not refer to the pupil by name.

Social networking and personal publishing

We are aware that bullying can take place through social networking.

The Academy will block/filter 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, Academy attended, Instant Messenger and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils and parents will be advised that the use of social network spaces outside the Academy brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or Academy attended.

Blogs or forums, used for educational purposes, will be delivered through the learning platform once it is introduced and permissioned to specific users or groups of users.

Teachers will be advised not to run social network spaces for student use on a personal basis. This will include sending of personal e-mails and IM. Staff should not allow “friend” access to their personal social networking spaces to pupils, former pupils or minors. They should ensure that communications with minors comply with their professional role. Abuse of this may result in disciplinary action being taken.

Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

Pupils will be advised not to publish specific and detailed private thoughts.

Anti-radicalisation and extremism

Radicalisation Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media in particular has become a major factor in the radicalisation of young people.

Extremism is defined by HM Government as 'Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs; and/or calls for the death of members of our armed forces, whether in this country or overseas'.
At Landau Forte Academy Moorhead we recognise that safeguarding against radicalisation and extremism is no different from safeguarding against any other vulnerability.
Our curriculum promotes respect, tolerance and diversity. Children are encouraged to share their views and to understand that they are entitled to have their own different beliefs which should not be used to influence others. We work hard to promote a culture of respect and responsibility and promote children's rights in our school. We have explored what Fundamental British Values are and promote this through our diverse curriculum offer.
We recognise that children with low aspirations are more vulnerable to radicalisation and therefore we strive to equip our pupils with confidence, self-belief, respect and tolerance as well as setting high standards and expectations for themselves.
Children are taught throughout our school about how to stay safe when using the Internet and are encouraged to recognise that people are not always who they say they are online. We work closely with the Prevent Team who support our work with families and individuals where needed. They are taught to seek adult help if they are upset or concerned about anything they read or see on the Internet.

Any concerns about pupils becoming radicalised or being drawn into extremism will be reported to the DSL who will *not* speak to parents/carers or other family members at this stage but will take prompt advice from the Police by contacting First Contact or the Prevent Team

Managing filtering

Internet filtering is delivered through a filtering system called Smoothwall. This delivers blocking strategies to prevent access to a list of unsuitable sites. Maintenance of the blocking list is maintained by Network administrators.

Access monitoring (via Smoothwall) records the Internet sites visited by individual users and are available to the Academy if needed.

The Academy will ensure that systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety coordinator.

Senior staff in conjunction with the technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

Pupil's Mobile phones are only allowed in the Academy in exceptional circumstances. They are given to the Administration Team at the beginning of the day and collected at the end of the day. The Academy will investigate infra-red and Bluetooth communication technologies and decide a policy on phone use in school when appropriate.

The use by pupils of cameras in mobile phones will be kept under review.

Staff must only use an Academy digital camera to take photos of children. Staff will not take photographs of pupils on their mobile phone or personal digital camera and must not download photos of the pupils onto their own PC or laptop. Students should never take images of children without the prior knowledge and consent of the teacher. Where photographs are transferred on to either their own lap top or memory sticks, these should be password protected. Any images taken must be shared with appropriate personnel before leaving the premises and the purpose of taking them discussed.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Please refer to the Academy's Data Protection policy for details.

POLICY DECISIONS

Authorising Internet access

All staff must read and sign the Staff Code of Conduct for ICT before using any Academy ICT resource. The Academy will maintain a current record of all staff and pupils who are granted access to the Academy ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Any person not directly employed by the Academy will be asked to sign an acceptable use of Academy ICT resources before being allowed to access the internet from the Academy site.

Assessing risks

The Academy will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the Academy network. The Academy can't accept liability for any material accessed, or any consequences of Internet access. The Academy will audit ICT use regularly to ensure the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling Online Safety complaints

Complaints of Internet misuse will be dealt with by a member of the Academy Leadership Team. Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be dealt with in accordance with the Academy child protection procedures.

Pupils and parents will be informed of the complaints procedure (see the Academy complaints policy).

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Discussions will be held with the Derby Safeguarding Children's Board when handling potentially illegal issues.

Introducing the Online Safety policy to pupils

Online Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and internet use will be monitored and appropriately followed up. A programme of training in Online Safety will be developed, some based on the materials from CEOP and Think U Know.

Online Safety training will be embedded within the Personal Social and Health Education (PSHE) curriculum, Anti-Bullying week and reinforced regularly when children have access to the Internet in the Academy. The Academy will also take part in the annual 'Safer Internet Day'.

Staff and the Online Safety policy

All staff will be given the Academy Online Safety Policy and its importance explained.

Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

The ICT technicians will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the Academy Online Safety Policy in newsletters, the Academy brochure and on the Academy website.

The Academy will maintain a list of Online Safety resources for parents/carers.

The Academy will ask all new parents to sign the consent form when they register their child with the school.

Internet issues will be handled sensitively, and parents will be advised accordingly.

A partnership approach with parents is encouraged. This will include parent evenings with demonstrations and suggestions for safe home Internet use.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents via parent meetings.

APPENDIX 1:

ONLINE SAFETY RESOURCES

Kidsmart: Kidsmart is an award winning practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Childnet International.

Hector's World: An excellent website that outlines all the dangers to children online and how to tackle each one in turn. Aimed at parents but equally relevant for teachers.

Child Exploitation and Online Protection Centre: The Child Exploitation and Online Protection (CEOP) Centre works across the UK and maximises international links to deliver a holistic approach that combines police powers with the dedicated expertise of business sectors, government, specialist charities.

Get Safe Online: Get Safe Online will help you protect yourself against internet threats. The site is sponsored by government and leading businesses working together to provide a free, public service.

Getting Your Head Around Internet Safety: An animated presentation on internet safety, with sound, from Parent's Centre and Childnet International.

Parents Centre Web Site: An excellent website that outlines all the dangers to children online and how to tackle each one in turn. Aimed at parents but equally relevant for teachers.

Think U Know: This website is created by the Child Exploitation and Online Protection (CEOP) Centre and contains loads of information on how to stay safe online. All hot topics are covered – including mobiles, blogging and gaming sites.

Signposts to safety: Teaching Online Safety at Key Stages 1 and 2: An excellent website that outlines all the dangers to children online and how to tackle each one in turn. Aimed at parents but equally relevant for teachers.

Digizen: An excellent website that outlines all the dangers to children online and how to tackle each one in turn. Aimed at parents but equally relevant for teachers.

Radicalisation and extremism:
http://www.internetmatters.org/issues/radicalisation/?gclid=CMfi6LjKycoCFUlmGwodvkAADA An informative website regarding the signs of Radicalisation and Extremism

APPENDIX 2

STAFF CODE OF CONDUCT FOR ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign a code of conduct. Members of staff should consult the Academy's Online Safety policy for further information and clarification.

This staff code of conduct provided by Landau Forte College, Derby (see attached).