On-line Safety Policy

Review Date: Spring 2019

Policy Title	**On-line Safety Policy**

Function	For Information and Guidance
Status	Recommended
Audience	Parents, Governors, Principal, Senior Leadership Team, Teachers, Business Support Staff
Implementation	The Principal and Governing Body have overall responsibility for ensuring that this policy is implemented
Version	V 1.0
Date Issued	Spring 2014
Date Approved by Governing Body	
Date for Review	Spring 2019

The Ferrars Academy
On-line Safety Policy

The On-line Safety policy is part of the Computing and Safeguarding policies. It also links to other policies including those for behaviour, anti-bullying, personal, social and health education and for citizenship. The policy provides an opportunity to review practice. It will aim to increasingly involve all children, parents, staff and Governors.

The Ferrars Academy On-line Safety policy has been agreed by the On-line Safety Co-ordinators (SLT) and Computing Co-ordinators (SLT) and Governors.

Rationale:

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Responsibilities

Governing Body / Principal Responsibilities

It is the responsibility of the Governing Body to both adopt and review this policy on an annual basis and to advise the Principal of any required changes.

It is the responsibility of the Principal to publicise and make this policy available to all current and future academy staff, and to ensure that the standards within it are both monitored and enforced and to advise the Governing Body of any serious breaches of this policy.

It is the responsibility of both the Principal and the Governing Body to take corrective and disciplinary measures as are necessary when a breach of this standard occurs and to contact and co-operate with police and other law enforcement agencies where a breach of these standards constitutes a criminal act.

All academy staff responsibilities

Employees must adhere to these standards in following circumstances:

- When working on academy premises
- When using equipment and utilities (hardware, software or mail and internet access) provided by the Academy at home or other locations

The standards apply regardless of whether access occurs during or outside of contracted work hours.

Employees must alert the Principal or a relevant senior member of staff where breach of these standards is suspected or known to have occurred.

INTERNET USE

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries
- Vocational, social and leisure use in libraries, clubs and at homes between pupils worldwide
- Educational and cultural exchange
- Internet use will be planned which will enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children
- Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Children will be taught to question what they read and seek confirmation from more than one source. Pupils will also be taught to respect copyright when using internet material in their own work
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administrative date with the Local Authority and SIMS
- Access to learning whenever and wherever convenient
- Offers opportunities for mentoring pupils and providing peer support for them and teachers
- Prepare the pupils for life beyond the classoom

Managing Information Technology Systems

The SLT will liaise with the ICT Technician and Interm IT to ensure that the systems in place in school are rigid and current. We will take regular advice from them. Interm IT will review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Internet Security

Local Area Network (LAN) security issues include:

- Users must take responsibility for their network use
- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive
- Servers must be located securely and physical access restricted from non authorised people.
- The server operating system must be secured and up to date
- Virus protection for the whole network must be installed and current

- Access by wireless devices must be proactively managed.

In addition to these measures Interm IT, our external technical support company will:

- review the security of the school information systems and users will be regularly reviewed.
- ensure virus protection will be updated regularly.
- ensure software cannot be installed or downloaded without administrator rights.
- ensure the files held on the schools network will be regularly checked.
- will review system capacity regularly.

How filtering is managed

Levels of Internet access and supervision at the Ferrars Academy will be regularly checked by the ICT Technician or Interm IT to provide the maximum amount of security.

The school works in accordance with RM who liaises with Interm IT for the filtering system within our Broadband.

If pupils discober unsuitable sites they click on Hector Protector and report it to an adult. If staff or visitors discover unsuitable sites, the URL (website address) must be reported in the website block file and blocking will take place via the ICT Technician or Interm IT. The person reporting the unsuitable site must write their findings in the ICT Concerns File which is located in the Computing Suite. If appropriate staff will be informed of any changes made to heighten security. If relevant, parents/carers will be informed of the matter sensitively.

The school will follow Luton's On-line Safety Guidance procedure if the issue is illegal.

How email is managed

Email is an essential means of communication for staff.

E-mail is an essential means of communication within education.

- E-mail must only be used in the academy with the children for educational purposes.
- All staff email accounts have a disclaimer on the footer.
- In-coming e-mail will be regarded as public. Received e-mail may be examined and could, for example, be pinned to a notice board.
- Messages sent using the academy domain name should be regarded in the same way as messages written on academy headed paper.
- All staff will be given an academy email address which is not to be given out to pupils.
- The forwarding of chain letters will be banned.
- Staff are reminded to be vigilant when opening emails.
- Children will be taught the Purple Mash email system and staff use Microsoft and Office 365 in the academy. This allows them to learn the skills of email but only

sends them internally within the academy environment. They will be taught about the effectiveness of communication and online bullying issues.

Children's emails will be reviewed regularly by the ICT Technician, to ensure the content is appropriate.

Managing social networking, social media and personal publishing

Each member of staff must have read and signed the academy Social Networking policy which outlines specific guidelines which need to be adhered to.All staff should be aware of the potential risks of using social networking sites or personal publishing.
The academy does not allow access to social media and social networking sites for staff or pupils whilst onsite, except the designated staff (Hazel Kelly HLTA and Sarah Green Acting Head) who publish updates on the academy facebook and twitter account.
The academy does not consider it has a responsibility to monitor the personal accounts of members of staff.

Managing Academy Website

Only specific authorised members of staff have access to edit / amend / publish content on the Academy website (Acting Head Sarah Green, Hazel Kelly, Beverley Johnson and Richard Brazauskas).

Editorial guidance will ensure that the academy ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure all information is considered from a security viewpoint including the use of photographic and video material.

Parents must sign the parental consent form for photographs of pupils to be used. If a child does not have consent then the academy is responsible for ensuring that no photographs of the child are used.

The point of contact on the academy website will be the academy address, academy email and telephone number. Staff or pupils personal information will not be published.

Our website has been built using the company E4Education and is reviewed in house by ICT Support and is managed by SLT.

Use of Pupil Images

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.
Publishing of pupils full names with their images is not acceptable.
Strategies include using relatively small images of groups of pupils and possibly even using images which do not show faces at all. Pupils in photographs should be appropriately clothed.
Images of a pupil should not be published without the parents or carers written permission.

Mobile Phones

Staff are not permitted to use mobile phones in the academy during the core day in front of children. They must be switched off, except during staff designated break times. On these occasions phones should not be used unless in the staff room or outside the building.
Visitors to the academy are reminded that phones should be switched off during meetings and should not be used at all if contact with children is involved.
At any time a member of the SLT can use their own discretion to allow mobile phones to be used on site by visitors or staff.
The only exception to the above points is for the Site Agent, who has a mobile phone which the academy has bought and it does not have a camera feature.
There is also a separate academy mobile phone which can be taken on educational visits which does not have a camera.

Introducing the policy to pupils

We follow the UK Council for Child Internet Safety policy – Click Clever, Click Safe code (Zip it, Block it, Flag it). Parents and children have access to documentation from school on this code of practice, which is available on request or downloadable from the website. Installed on the schools computer is a programme called Hector Protector from the website www.thinkuknow.co.uk. Children are taught what to do if they see something on their screen which they are concerned about. Our school website has a page linked to lots of different On-line Safety pages for both children and adults to look at, which is regularly reviewed.

- Rules for Internet access and SMART (Safe, Meet, Accepting, Reliable, Tell) posters will be displayed in all rooms where computers are used.
- Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the internet.
- Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.
- Acceptable User Agreement will be shared with pupils at the start of year and relevant points throughout each term. The agreement will also be sent home to be reinforced with their child.
- Assemblies ½ termly
- Introducing the policy to parents
- Parent workshops, Newsletters and specific letters, magazines such as digital parenting.

Photographic, video and audio technology

- Staff are not permitted to use their mobile phones during the academy day unless on a break and only used in the Staff room. They must be switched off at all times.
- The Academy's ICT equipment must be used on trips and at events. Staffs personal cameras must not be used.
- Parents are to give consent for photos and video to be used for academy purposes.
- Webcams will only be used in the presence of a teacher.

Conducting financial activities on the internet

While this policy does not specifically ban the use of the internet for conducting personal financial transactions e.g. E-banking, we warn against it. Residual information from such activities can be left on your computer hard drive and could subsequently be accessed by others. The Academy does not accept any liability for any resulting loss or damage. When purchasing items for the academy online caution should be used in the safety of websites and the appropriate pre-purchase forms completed before a transaction is made (file in Business Managers Office).

Electronic Communication

Currently we use an online texting service (School Comms) via the internet which can be accessed remotely by nominated people at home and school and is a password protected site.

How personal data is protected at The Ferrars Academy

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure all personal information is handled properly. It promotes openness in the use of personal information. Under the act every organisation that possesses personal information (personal data) must notify the Information Commissioner's Office, unless exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when possessing personal data. The Act also gives rights to the people the information is about ie subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

The school will take all reasonable precautions to ensure that users access only appropriate material.

Encrypted USB Sticks

Each member of staff / Governor is issued with an encrypted usb stick. They sign an agreement to acknowledge that any documents or information relating to the Academy, staff or pupils must be stored securely on this stick and on no other devices.

Mobile Technology

All teaching staff are issued with a laptop and ipad mini to assist with educational purposes. Devices are all password protected to ensure confidentially of documents.

Staff are allowed to take ipad minis off site.

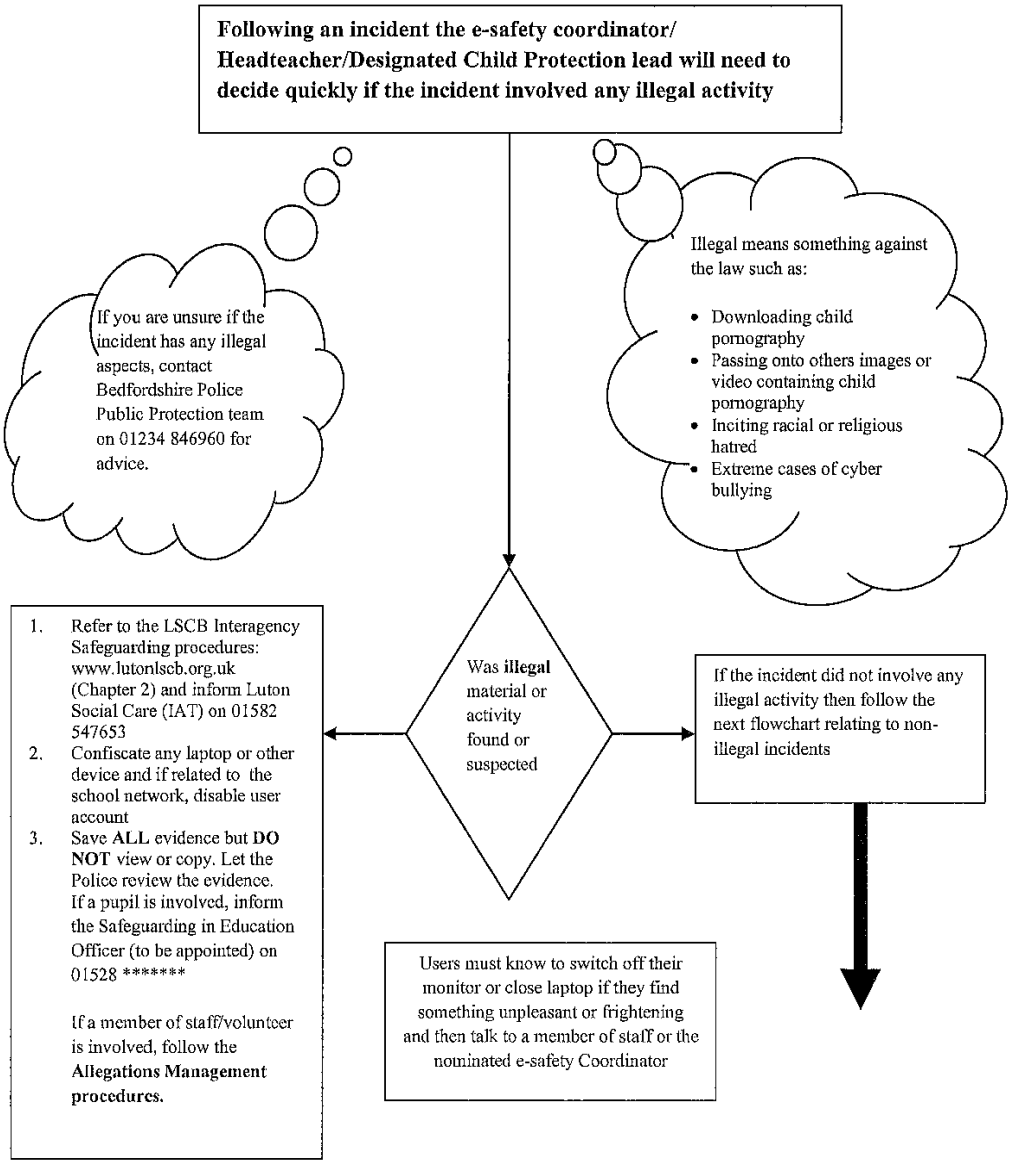
Community Use / The Wider Academy Environment

- Academy computing resources may be increasingly used as part of the extended school agenda.
- Adult users of our school network will sign the academy acceptable user agreement.
- The Academy will make Information and Guidance for parents on On-line Safety available in a variety of formats.

Spring 2017

Review Date: Spring 2019

Luton flowchart to support decisions related to an illegal e-safety incident for Headteachers, Senior Leaders and e-safety coordinators



Luton flowchart to support decisions related to non-illegal e-safety incident for Headteachers, Senior Leaders and e-safety coordinators