Keelman's Way School

E-Safety and Acceptable Use Policy

Introduction

Rapidly developing information and communication technologies (ICT) are exciting and motivational learning tools through which learning and teaching can be greatly enhanced. This policy is a direct response to DFE and Ofsted safeguarding and inspection criteria and therefore creates a framework for our school to ensure ICT is being used safely and responsibly and that the risks relating to ICT use are properly managed.

Contents

Roles and Responsibilities

Keelman's Way has adopted a whole school approach to e-Safety (although overall responsibility rests with the Head Teacher and the Governing Body), which aims to ensure that there are plans in place to revisit and reiterate to all staff their responsibilities for e-Safety, as well as understanding the roles of designated individuals with e-Safety responsibilities.

The Head Teacher and ICT Co-ordinator have access to monitoring reports, should a violation be highlighted, efforts will be made to trace the perpetrator or the person/student responsible. Incidents will be recorded in the internet log book which is kept in the school office.

The role of Network Manager is held by the school Technician who is responsible for some critical elements of e-Safety procedures. The role and responsibilities of the Network Manager include the following:

- The oversight of the network.
- Monitoring the performance of the network.
- Ensuring the network is secure.
- Detecting errors and acting accordingly.
- Implementing access controls.
- Installing and removing software.

Internet Use

The broadband service at Keelman's Way is provided by BT.
Internet use is part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning.

- The school Internet access will be designed expressively for student use and will include appropriate filtering.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

E-mail by pupils

- Students may only use approved e-mail accounts on the school system.
- Students must immediately inform an adult if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail by staff

- All external e mails sent by staff will include school signature.

- Only Office 365 may be used by staff on school lap tops, (inc. lap tops provided for teachers).
- Discuss other members of staff or students in a negative fashion in a public space on the internet goes against the 'Code of Conduct' and does not treat people with respect and courtesy.
- All staff have the responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people.

Communication with Children and Young People

- Communication between children and adults by whatever method should always take place with clear and explicit professional boundaries.
- Staff must not share any personal information with any young people or children. They must not respond to requests or request any personal information from the child/young person, other than that which may be appropriate as part of their professional role.
- Staff will ensure that all communications are transparent and open to scrutiny.

Mobile Phone Usage

Students are not allowed mobile phones or mobile devices in school. Should a student have a device it must be handed to a member of staff for safe keeping and is returned to them at the end of the school day.

Staff use of mobile phones:

- Personal mobile phones must not be carried around school in pockets or bags, but kept securely.
- Personal phone calls or sending of text messages should only be made outside of teaching hours unless express permission is given from senior manager.
- The taking of pictures from a mobile phone on Keelman's Way premises and trips outside of school is unacceptable. School iPod's should be used.

Access to the Network

All staff have unique user names and passwords which allow them access to staff shared areas as well as more general areas. Pupil's access is limited to a pupil shared area and learning tools. Guest and visitors to the school may be issued a username and password with access levels appropriate to their needs.

Social Networking

Adults will:

- Uphold the law and maintain a good standard of behaviour both inside and outside of school; both online and offline. The content in cyberspace does not elude the law – a posting in the public domain can still constitute a defamatory publication. Employers can take disciplinary action if they prove your conduct has caused detriment.
- Note that they may lose respect in their post and deformation of character by placing things in the public eye that relate to their role or other members of staff.

- Members of staff must not become ‘friends’, ‘link’ with or follow parents or guardians of children at Keelman’s Way on social networking sites. It will be made clear to parents that this is inappropriate. Such requests must be mentioned to a line manager.
- In all instances, not disclose anything on social networking sites that are related or could be related back to their work. If it is necessary to disclose information by these means it is advised to do so via private means and not, for example on a ‘Face Book’ wall.

Propriety and Behaviour

Adults will not:

- Place images and videos of themselves on a public space on the internet such as ‘You Tube’, or ‘Facebook’, which could show themselves or other members of council staff in a way which could damage the council’s reputation must be avoided and the council will take seriously any action deemed to show a lacking in standards both online and offline.
- Any unauthorised contact between parents and members of staff at Keelman’s Way must be recorded on an incident form.

Communication with Children and Young People

- Communication between children and adults by whatever method should always take place with clear and explicit professional boundaries.
- Staff must not share any personal information with any young people or children. They must not respond to requests or request any personal information from the child/young person, other than that which may be appropriate as part of their professional role.
- Staff will ensure that all communications are transparent and open to scrutiny.

School website

The School website is managed by Sara Padden and Trevor Heron. Staff provide items for uploading, all pupils have received a letter requesting permission for their photographs to be used. Those without parental permission are noted.

Passwords

All access to ICT systems by staff is via a login and password. Access credentials (usernames and passwords) should not be generic and should be changed frequently (at least termly) to protect ICT systems. All staff should be made aware that access credentials should not be stored within the machines, internet browser or any remote access software.

Staff

- Staff are made aware that any software provided by the workplace can only be used by members of staff and only for educational use.
- Staff are not to leave any information system unattended without first logging out or locking the computer as appropriate.
- Staff will respect the system security and will not disclose any password or security information.
- They are to use a 'strong' password that contains numbers, letters and symbols, with 8 or more characters.

Pupils

- Due to the complex needs of our children, all pupils will log on using the same user name and password. Older/more able students will be given individual user names for certain activities, e.g. sending e –mails.
- Pupils must be supervised at all times when using the internet.
- All machines are logged using Securas and individual machines can be tracked if anything inappropriate is viewed/searched for using the internet. Staff are able to identify specific pupils that are using the machines at the time.

Use of ICT systems

In order to achieve Network Security internet usage will be filtered by an approved smart filter. Staff and pupils will be made aware that all school ICT activity and on-line communications may be monitored, including any personal and private communications made by the school network.
E safety education is a crucial part of using technology and at Keelmans Way we take this very seriously.

- e-Safety education will be regularly re-visited by Staff and Students ensuring that coverage will meet the National Curriculum 2014 for Computing and the EQUALS schemes of work.
- School Workforce training in understanding the rationale for all e-Safeguarding procedures and the consequences of inappropriate practices.
- School Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as photographs and videos in terms of permission seeking, taking, storage and retention.
- Personal internet use by staff is only permitted during non- teaching times, e.g. before/after school or during break times. Staff are to access the internet through their personal accounts and children are not to be present.

Incident Reporting

An important element of e-Safeguarding is the ability to identify and deal with incidents related to Information Security breaches and the online safety of pupils and staff.
All staff and pupils have a responsibility to report e-Safety or e-Security incidents, this includes websites that are deemed inappropriate and cyber bullying, so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the school.
An incident log will be kept to ensure it captures the following information:

- Incident Date
- Description of the Occurrence
- Immediate Corrective Action
- Further Action
- Legal Implications
- Closed Date

The ICT Coordinator will hold and monitor the incident log and all staff and pupils will be made aware of the importance and their responsibility in reporting incidents. All pupils are aware that they are monitored when using the internet and are aware of the importance of staying safe by taking part in activities related to e-safety which is included in the curriculum. Pupils are aware of who they would approach if a problem were to arise, e.g. they have a trusted adult they would go and speak to.
The incident log will be formally reviewed and any outstanding actions delegated by the Senior Leadership Team on a termly basis. If appropriate, management should update the Risk Assessment in the light of any new incidents. The log and accompanying action plans should be reviewed annually by the Governing Body.
If an incident is reported the review process will assess the risk associated with the incident, the implications to the organisation and the potential threat to pupils and staff.

Parents and Extended Schools

Every opportunity will be made to involve parents and other stakeholders. Parents will be signposted to particular websites and supported by staff to develop their own understanding of how to keep their children safe when using technology at home.

Starters and Leavers

All employees and pupils within school may have access to a range of important and sensitive information. It is essential that the integrity of the schools systems and information remain secure when users start with or leave the establishment. The following action should take place:

- User accounts to be disabled or removed as soon as they leave the school.
- Email accounts should be disabled or removed as soon as they leave service.
- Any learning platform access should be disabled as soon as they leave the school.
- Procedures should be followed for dealing with copyright of any files, programmes or data that are owned by the school.
- Images of pupils or staff that may exist on mobile devices should be removed within 24 hours and stored in the shared area in an identifiable folder.
- Password protected or encrypted data needs to be made available to staff within the organisation.

The above actions should be carried out regularly to manage the risk of unauthorised access to any internal data or systems.

Remote Access

The removal of any ICT equipment, information and software from school premises should only be permitted with authorisation from the ICT coordinator, Senior Information Risk Owner, or Head teacher.

- All users of mobile computing equipment are responsible for safeguarding such equipment.
- Responsible precautions should be exercised to prevent theft, loss or damage and to prevent unauthorised access.
- Devices which are left in cars, hotel rooms or the home should at all times not be visible and locked securely.
- Only necessary information should be stored on the device.
- Pupil’s sensitive information shall not be stored on any mobile devices unless encrypted, e.g. memory sticks.
- All staff have permission to take home school lap tops and iPad’s. They are made aware that even though they are off school premises internet activity is still tracked

through Securas. If staff allow family members use the internet on school laptops/ iPad's they are held responsible for any unacceptable use of the internet.

Technical Security

The technical support staff within school will ensure that all machines joined to the network have all the applicable security software installed on them.

- All desktops shall have up to date anti-virus software installed.
- All incoming email shall be scanned for viruses and filtered for spam.
- All virus definitions shall be updated daily.
- All anti-virus shall be configured to alert the technical support team when any virus is detected.
- Where possible, the use of memory sticks and other mobile storage media should be restricted, or scanned for viruses each time they are connected.

Training

Staff receive regular updates on E safety issues from the ICT Co-ordinator and LA staff. Senior staff attend LA briefings and feedback to the school. `

Signed ……. Date Spring 2017 Review Spring 18
Head Teacher

Signed ……. Date ……
Chair of Governors