Category	Security		
Document Name	E-Safety Policy		
Accountable Body	RADIUS Trust		
Reference	SY.P2	**Date Ratified**	11th December 2014
Version	3.1	**Last Update**	31st March 2015

Related Documents

Document	Reference
Protocol for Acceptable Use of Internet and Email by Staff	SY.P2.T1
E-Safety Procedures	SY.P2.01
Safeguarding & Child Protection Policy	SC.P1

Reference Material

Guidance
Data Protection Act 1998
DfE Cyberbullying: advice for Headteachers and school staff Nov 2014
DfE Advice for parents and carers on cyberbullying Nov 2014

1. Scope

This policy applies to all members of each school community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both on and off school premises.

The Education and Inspections Act 2006 empowers the Trust, as Accountable Body to delegate to its Headteachers / Principals to such 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 exercised by the Trust via its Headteachers/Principal with regard to the searching for and of electronic devices and the deletion of data.

The Trust expects each school to address incidents of breaches of standards and practices with regard to e-safety through local management and professional action with pupils and adults having regard to associated behaviour management processes and procedures and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

2. Policy Statement

The Trust expects internet access and capability in each school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

The Trust and its schools aim to equip the pupils with all the necessary ICT skills for modern life.

Some of the benefits of using ICT and the internet in schools are:

RADIUS Trust
Registered Charity Number: 1039938
Company Registration Number: 2919225
Registered Office: Trust Office,
Horsham Road, Grafham, Bramley,
Guildford, Surrey GU5 0LH

Pupils

- Access to worldwide educational resources and institutions to support all aspects of the curriculum and associated learning activities.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom or similar learning setting.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

Employees

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and learning settings strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to pupils and parents.
- Class/learning activity management, attendance records, schedule, and assignment tracking.

Authorising Internet Access

- All employees are required to read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource (refer to SY.P2.T1 Protocol for Acceptable Use of Internet and Email by Staff)
- All pupils and employees are required to have a regulated set of passwords with unique identifiers and recorded as assigned to individuals.
- Pupils access to the internet will be in supervised activities with access to specific, approved on-line materials.

Assessing Risks

Schools are expected to take all reasonable precautions to prevent access to inappropriate material.

Each school is expected to have a procedure and system in place to monitor ICT use to establish if the e-safety procedure is adequate and that the implementation of the e-safety policy and related procedures are appropriate and effective.

Roles & Responsibilities

Each school's Governing Body is responsible for the approval of the school's procedures related to this E-Safety Policy and for reviewing the effectiveness of those procedures. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Each Governing Body is expected to have within its lead governor portfolio a degree of awareness and oversight of the adequacy of schools systems to ensure e-safety. Unless otherwise provided for the Lead Governor will be assumed to be the lead governor for Safeguarding and Child Protection. The governor oversight role may include:

- regular meetings with the school's E-Safety Co-ordinator ;
- validation that the school has regular monitoring of e-safety incident logs in place;
- Validation that the school has in place regular monitoring of filtering / change control logs.

Each school is required to clearly identify the roles and responsibilities in relation to e-safety:

- Headteacher / Principal and Senior Managers.
- E-Safety Coordinator with specific roles and responsibilities for e-safety procedures.
- Teaching and Support Staff – especially staff involved in supervising residential provision.
- Safeguarding & Child Protection Designated Person.
- Pupils / Students.
- Parents / Carers.

The Trust IT Manager or school's IT specialist employee/agent is 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 the Trust's E-Safety Policy;
- that users may only access the networks and devices through a properly enforced password protection procedures, in which passwords are regularly changed;
- the filtering procedures are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Principal; E-Safety Coordinator for investigation / action / sanction;
- that monitoring software / systems are implemented and updated as agreed in school procedures.

3. Teaching and Learning

The Trust requires each school to clearly outline the use of ICT within the school's curriculum and the benefits to teaching & learning. The school procedures are expected to identify the control measures in place to reduce risk involved in the use of ICT within the curriculum as well as sanctions in the event of an incident.

Both pupils and their parents/carers are required to sign a Home School Agreement (or similar arrangement) to ensure they have read, understood and agreed to the E-Safety rules as outlined in the school's E-safety procedures.

4. Web Filtering

Filtering strategies are selected by each school, in discussion with the Trust's IT Manager employed via the Charity Office. The filtering strategy is selected to suit the age and curriculum requirements of the pupil.

Any material found that is believed to be unlawful will be reported to the appropriate regulatory agencies.

Managing Information Systems

The Trust IT Manager is charged with establishing and maintaining effective web filtering technology and systems to support each school to maintain effective e-safety infrastructure.

The security of each school's information systems and users will be reviewed regularly by the IT Manager and virus protection software will be updated regularly.

The Trust requires the following systems to be in place and adhered to:

- ensuring that all personal data sent over the internet or taken off site is encrypted;

- making sure that unapproved software is not downloaded to any school computers;
- files held on the school network will be regularly checked for viruses;
- the use of user logins and passwords to access the school network will be enforced.

5. Emails

Each school and the Charity Office are expected to comply with the Trust's Data Security, Protection & Retention Policy and to inform staff that schools email accounts are only to be used for Trust / school-related matters, i.e. for staff to contact parents, pupils, other members of staff and other professionals for work purposes. The school has the right to monitor emails and their contents (refer to SY.P2.T1 Protocol for Acceptable Use of Internet and Email by Staff).

6. Published Content and Websites

All websites operated in the name of the Trust including school specific pages and presence are required to comply with the highest standards of content maintenance.

Any information published on the website is to be carefully considered in terms of safety for the pupils, staff, copyrights and privacy policies. No personal information on staff or pupils is to be published and the only contact details for contacting the school will be via the school office or authorised staff school email addresses.

The Headteacher / Principal and as delegated to a named school Website Administrator (or Charity Office Manager in the case of the Charity Office) will take overall editorial responsibility and ensure that content is accurate and appropriate. Cross reference is required with the Trust's Data Security, Protection & Retention Policy especially relating to web posting of pupil images.

7. Social Networking and Social Media

Online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. The Trust requires each school to educate pupils so that they can make their own informed decisions and take responsibility for their conduct online and have clear procedures in place with respect to social media.

Each school's procedures are required to clearly state that pupils are not allowed to access social media sites in school.

Employees should restrict use of social media to personal uses only. Personal use of social media should refrain from reference to employment activity and school life. Employment related potential use should be approved by the Headteacher/Principal of the school or a direct senior line manager. Further information is available in SY.P2.T1 Protocol for Acceptable Use of Internet & Email by Staff.

8. Mobile phones and personal data devices

While mobile phones and personal communication devices are commonplace in today's society, each school is expected to be aware of their use and ensure that mobile phones are used responsibly.

9. Handling E-safety Incidents

The Trust requires each school's procedures to include clear instructions for all E-safety incidents including the roles and responsibilities to record the incident, agree an action and monitor and review the incident. Depending on the severity of the incident, other parties may need to be involved at the discretion of the Headteacher/Principal and the school's designated person for Safeguarding & Child Protection.

10. Cyberbullying

The anonymity that can come with using the internet increases the confidence in individuals to say and do hurtful things that they otherwise would not do in person.

Information about specific strategies or programmes in place to prevent and tackle bullying is to be set out in the schools Behaviour Management procedures. It is to be made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in an investigation by senior staff.

The Trust and each school have a statutory duty to look after the physical and mental health of its employees. This includes protecting staff from cyberbullying and supporting the individual in the event of an incident. Each school is expected to:

- make staff aware of the potential risks of being bullied online through social networking sites by parents/carers and pupils
- train staff on how to protect themselves from cyberbullying
- ensure staff are aware on how to report incidents of cyberbullying and provide advice and support to the individual throughout the process

Further information can be found from the DfE guidance 'Cyberbullying: advice for Headteachers and school staff Nov 2014'.

11. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. Each school is required to risk-assess any new technologies before they are used and ensure the technology provides educational benefits. Each school is expected to keep up-to-date with new technologies and to be prepared to quickly develop appropriate strategies for dealing with new technological developments.

12. Monitoring

The Trust requires each school to monitor any concerns relating to e-safety by:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity.

Additionally the Trust expects a lead governor with a portfolio which includes e-safety to be kept apprised of issues and management action to ensure e-safety maintenance.

13. Parent Advice

Parents/carers play a vital role in the safety of children and young people online and each school is expected to provide guidance on e-safety through the following:

- Home School Agreement - ensure parents/carers understand the school's e-safety rules and procedures.
- School website – provide links to validated third party advice on e-safety and publish DfE guidance such as 'Advice for parents and carers on cyberbullying Nov 2014'.