RIPLEY ST THOMAS
A CHURCH OF ENGLAND ACADEMY

E-Safety Policy

Originator	G Gomersall
Reviewed	May 2016
Next Review Date	May 2018

Ripley St Thomas
Ashton Road
Lancaster
LA1 4RS

t 01524 64496 **f** 01524 847069
e admin@ripley.lancs.sc.uk

website: www.ripleystthomas.com

Believe.....

E-Safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The academy's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure academy network design and use.
- Safe and secure broadband from Virtue Technologies including the effective management of filtering via Sophos Unified Threat protection (UTM), Sophos Network Protection and Sophos Web Protection.
- National Education Network standards and specifications.

Further Information

Further information is available from the websites below. If you wish to contact our eSafety co-ordinator, then please complete the ParentLine form at http://ripleystthomas.com/contact/#parentline

Think U Know website	www.thinkuknow.co.uk
Becta e-Safety	www.becta.org.uk/schools/esafety

Academy e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the Academy Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The academy will appoint an e-Safety coordinator. In many cases there will be overlap with the Designated Child Protection Officer. In matters of Child Protection the Designated Child Protection Officer's judgements outweigh those of the e-Safety co-ordinator.
- Our e-Safety Policy has been written by the academy, building on government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed tri-annually.

2.2 Teaching and learning

2.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide students 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.

2.2.3 Internet use will enhance learning

- The academy 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.2.4 Pupils will be taught how to evaluate Internet content

- The academy will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Internet Access

2.3.1 Information system security

- Academy ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be reviewed in line with the issuing of guidance from the Department for Education (DfE) and other safeguarding bodies.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the academy system.
- 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 an external organisation should be written carefully before sending, in the same way as a letter written on academy headed paper.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the academy website

- The contact details on the Web site will be the academy address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupils images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Parents will be informed that photographs of their child/children may be used on noticeboards around the academy, in academy newsletters and other printed materials. Parents will also be informed that photographs may be used on the academy website. These pictures will not be accompanied by names.
- Work may be published without the permission of the pupil and parents.

2.3.5 Social networking and personal publishing

- 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 or their location. Pupils are advised not place personal photos on any social network space. Pupils must not place personal photographs of them in academy uniform on any social network space or other.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.

2.3.6 Managing filtering

- The academy will work in partnership with the DfE and Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to a teacher, e-Safety Coordinator or the Network Manager. Teachers should inform the e-Safety Coordinator. The academy will make a decision regarding reporting this to the relevant agencies e.g. CEOP, Police or IWF.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils will ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

2.3.8 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.
- Generally, mobile phones will not be used during lessons or formal academy time. Small exceptions may exist for Computer Studies where the content of the lesson involves designing and creating applications for smart phones. Further details are available in the Mobile Phone Policy. The sending of abusive or inappropriate text messages (SMS / MMS) or images is forbidden.
- Staff will be issued with an academy phone where contact with pupils is required.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Cyber Bullying

2.4.1 Cyber-Bullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in the academy. Full details are set out in the academy's policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by Cyberbullying.
- All incidents of cyberbullying reported to the academy will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

2.5 Policy Decisions

2.5.1 Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any academy ICT resource – see page 11
- The academy will maintain a current record of all staff and pupils who are granted access to academy ICT systems.
- All pupils must apply for Internet access individually by signing a form stating they agree to comply with the e-Safety Charter and e-Safety Rules.
- Parents will be asked to sign and return a consent form.

2.5.2 Assessing risks

- The academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. The academy will not accept liability for the material accessed, or any consequences of Internet access.
- The academy will periodically audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

2.5.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the e-Safety Officer.
- Complaints of a child protection nature must be dealt with in accordance with the academy's child protection procedures.
- Pupils and parents will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.5.4 Community use of the academy's facilities

- The academy will liaise with local organisations to ensure they comply with the academy's e-safety policy when using academy facilities.

2.6 Communications Policy

2.6.1 Introducing the e-safety policy to pupils

- e-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.

2.6.2 Staff and the e-Safety policy

- The academy e-Safety Policy will be made available to all staff and its importance explained.
- Staff should be aware that Internet traffic and emails can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

2.6.3 Enlisting parents' support

- Parents' attention will be drawn to the academy e-Safety Policy in newsletters, the academy brochure and on the academy Web site.

Ripley St Thomas Church of England Academy

e-Safety Charter

You have the right:

- to enjoy the internet and the benefits it offers
- to feel safe when using computers and other technologies
- to be safe from online bullying and the right to report it
- to explore the internet and to question any information you find
- to keep information about you private and to tell people only what you want them to know about yourself
- to decide whether or not you wish to communicate with someone, either online or through other digital technologies
- to choose whether to fill out forms or answer questions you find on the internet
- to object to being filmed or photographed by anyone using cameras, web cams or mobile phones
- to object to any videos or images of yourself being placed on the internet, and to request that they are removed
- to object to your work being used by other people
- to be educated about safe use of the internet

You have the responsibility:

- to use the internet sensibly, legally and not to the detriment of others
- to use technologies legally and respectfully and to inform the relevant authorities, should you encounter inappropriate, illegal or harmful content
- to treat others with respect and to report online bullying; do this safely, sensibly and legally and check any information before using it
- to provide information that is not misleading, to keep your own data safe and not to misuse any information you have about others
- to be respectful when communicating with others electronically and you should always inform a responsible adult if something makes you feel uncomfortable or you become suspicious of another user's behaviour; do this accurately and legally
- to protect yourself, by behaving in a way that will avoid embarrassment when videos and photographs are being taken
- to use images and videos of yourself and others in a respectful and legal manner
- to ensure you have permission to use other people's work
- to put this education into practice both in and beyond the academy

Ripley St Thomas Church of England Academy

e-Safety Rules

These e-Safety Rules help to protect students and the academy by describing acceptable and unacceptable computer use.

- The academy owns the computer network and can set rules for its use. Pupils and parents agree that use of these facilities is bound by the rules of the academy.
- It is a criminal offence to use a computer or network for a purpose not permitted by the academy. Activity that threatens the integrity of the academy ICT systems, or activity that attacks or corrupts other systems is forbidden.
- Irresponsible use may result in the loss of network or internet access, which will be detrimental to the child's progress at academy.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and internet use must be appropriate to education and curriculum usage.
- All websites have to be approved by the Network Manager in conjunction with the internet provider before they can be used/accessed.
- The academy will endeavour to ensure that pupils and staff will only be able to access approved sites.
- Visits to unapproved sites by pupils will mean that the Principal and parents will be informed and the pupils will be locked out of the system. Visits to unapproved sites by teachers will be notified to the Principal and Governing Body for action.
- Copyright and intellectual property rights must be respected.
- Anonymous messages and chain letters are not permitted.
- When using e-mail, messages must be written carefully and politely, using high standards of language and appropriate content, particularly as email could be forwarded to unintended readers. All offensive words of any description are forbidden. All communications must comply with good equal opportunities and non-discriminatory practices. Students must use the academy email system to contact any member of staff and vice-versa.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging. Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- The academy ICT systems may not be used for private purposes, unless the Principal has given specific permission.
- Use for personal shopping, financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The academy may exercise its right to monitor the use of the academy's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the academy's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery, sound or other materials.

Dear Parent/Guardian

Ripley e-Safety and Internet Acceptable Use Policy

As part of the academy's ICT programme, we offer pupils access to the internet. Before the academy allows pupils to use these facilities, they must obtain parental permission. Both pupils and parents must signify their acceptance of the academy's e-Safety Rules.

Various projects have proven the educational benefits of internet access which enables pupils to explore a wide range of information sources throughout the world. Although there are concerns about children having access to inappropriate material via the internet, the academy takes a range of measures to minimise these risks. A filtering system is in operation which restricts access to inappropriate materials, and this is reinforced by the ICT staff who teach the safe and appropriate behaviours to adopt when using the internet, email and other technologies.

Although internet use is supervised and filtered within our academy, families should be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people. As with any other area, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources at home.

At the academy, teachers will guide students towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones and films.

We hope you will read through the attached E-Safety Rules & Charter with your child so they understand what is appropriate and acceptable in the academy.

Yours sincerely

I G Gomersall
Director of Operations

Ripley St Thomas Church of England Academy

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/guardians are asked to sign to show that the e-Safety Rules have been understood and agreed.

Name of Pupil:

Pupil's Agreement

- I have read and I understand the academy e-Safety Rules
- I will use the computer, network, internet access and other new technologies in a responsible way at all times
- I know that Network and internet access may be monitored

Signed: **Date:**

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and videos that include my son/daughter may be published subject to the academy rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the academy e-Safety rules and give permission for my son/daughter to access the internet. I understand that the academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the academy cannot be held responsible for the content of materials accessed through the internet. I agree that the academy is not liable for any damages arising from use of the internet facilities.

Parental Signature: **Date:**

Please print Parent/Guardian's Name:

Please complete, sign and return to the academy.

Ripley St Thomas CE Academy

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the academy's e-safety policy for further information and clarification.

- The information systems are the property of the academy and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that academy information systems may not be used for private purposes, without specific permission from the Principal.
- I understand that the academy may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in the academy, taken off the academy premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the academy e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils and staff are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The academy may exercise its right to monitor the use of the academy's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …….. Initials: …… Date: ……..

Accepted for the academy: …… Initials: ……..