RIPLEY ST THOMAS
A CHURCH OF ENGLAND ACADEMY

Online Safety Policy

Originator	A Korab
Reviewed	November 2018
Next Review Date	November 2020

Ripley St Thomas
Ashton Road
Lancaster
LA1 4RS

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

website: www.ripleystthomas.com

Believe.....

Index of content

1. Development / Monitoring / Review of this Policy

This Online Safety policy has been developed in consultation with:

- Senior Leaders
- Online Safety Officer
- Staff – including Teachers, Support Staff, Technical staff

Consultation with the whole Ripley community has taken place through a range of formal and informal meetings.

1.1 Schedule for Development / Monitoring / Review

This Online Safety policy was approved on:	*November 2018*
The implementation of this Online Safety policy will be monitored by:	*The Principal and SLT*
Monitoring will take place at regular intervals:	*Monthly*
The Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	*At least once a year*
The Online Safety Policy will be reviewed every two years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*November 2020*
Should serious online safety incidents take place, the following external persons / agencies may be informed:	*LA Safeguarding Officer* *LADO* *Police*

The school will monitor the impact of the policy using:

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

1.2 Scope of the Policy

This policy applies to all members of the Ripley community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of our ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Ripley site and empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for electronic devices and the deletion of data. In the case of both acts, action will be taken over issues covered by our Behaviour Policy and Mobile Devices Policy.

We will deal with such incidents within this policy and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Ripley academy:

2.1 Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of the Safeguarding Governor will include online safety.

2.2 Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including online safety) of members of our community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer.
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The DSL will receive monthly monitoring reports from the Online Safety Officer.

2.3 Online Safety Officer:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of who to speak to in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents to inform future online safety developments
- reports termly to Senior Leadership Team

2.4 Network Manager / Technical Staff:

The Network Manager is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to SLT or the Online Safety Officer for investigation.
- that monitoring software / systems are implemented and updated.

2.5 Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices.
- they have read, understood and signed the Staff Acceptable Internet Use Statement.
- they report any suspected misuse or problem to the Online Safety Officer or Pastoral leader for investigation / action / sanction.

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement our Mobile Devices Policy with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

2.6 Designated Safeguarding Lead :

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

2.7 Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand our Mobile Devices Policy. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

2.8 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and the academy website. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy (where this is allowed)

3. Policy Statements

3.1 Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of our academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the academy.

- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (via the online safety officer) can temporarily remove those sites from the filtered list for the period of study. Once the site is no longer required, staff should inform the Technical Staff (or online safety officer) and the site will be added back into the filtered list.

3.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and the web site
- Parents / Carers evenings / sessions

3.3 Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff. This will be regularly updated and reinforced through staff meetings.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Online Safety Officer will provide advice / guidance / training to individuals as required.

3.4 Training – Governors / Directors

Governors should take part in online safety training sessions, with particular importance for those who are members of any subcommittee involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in academy training.

3.5 Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and secure password by the network manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (eg academy safe)
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- Internet access is filtered for all users**.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users.
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- A system is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- A system is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

3.6 Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education programme.

3.7 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement strategies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, except in the media in accordance with consent given as part of Data Protection Act 2018/GDPR.

4. Data Protection

Below is a summary of the policy. For the full details, please refer to the Data Protection & Freedom of Information Policy.

Personal data will be recorded, processed, transferred and made available according to the GDPR and Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using secure cloud services.

When personal data is stored on any portable computer system or any other removable media:

- the data must be encrypted and sensitive data password protected.

- the device must be password protected and encrypted.
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

5. Communications

When using communication technologies the academy considers the following as good practice:

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Online Safety Officer or Data Protection Officer – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.

5.1 Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Academy staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school / academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the academy
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official academy social media accounts are established there should be:

- A process for approval by the online safety officer
- Clear processes for the administration and monitoring of these accounts – involving the online safety officer and the DPO
- A code of behaviour for users of the accounts which is discussed with the Online Safety Officer before accounts are made available
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

The academy’s use of social media for professional purposes will be checked regularly by the Online Safety Officer to ensure compliance with the school policies.