THE RUSSETT SCHOOL

# E SAFETY & ONLINE SAFETY POLICY

Written by ……………Jessica Whalley Date …… October 2017…….

Reviewed by …………. Andrew Howard Date …….. October 2018 ………
…

This is a non *statutory* policy and it will be reviewed/amended Autumn 2021

Document Control

There is one controlled copy of this document:

Copy 1 on Trust Governor

THE
RUSSETT
LEARNING
TRUST

Challenge for Achievement

Working in Partnership with

The Russett School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the academy community, but it is important that the use of the Internet and ICT is seen as a responsibility and that pupils/students, staff and parents use it appropriately and practice good online safety.

It is important that all members are aware of the risks associated with using the Internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities. Online safety falls under this duty. Staff will be reminded regularly about their responsibilities and to remain vigilant.

It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This strategy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our anti-bullying policy

## 1. Roles and Responsibilities

**The school Online Safety Coordinator is:** Miss J Whalley

**The Designated Safeguarding Governor is:** Mrs Frances Beck

**The Designated Safeguarding Lead is:** Mrs Kathryn Richardson

**The Deputy Designated Safeguarding Leads are:** Mr E Duffy & Mrs Catherine Lewis

### Board of Directors & Local Governing Committee

Online safety falls within the remit of the governor responsible for Safeguarding. The role of the Online safety governor will include:

- Ensure an Online Safety Strategy is in place, reviewed every year and is available to all stakeholders.
- Ensure that there is an Online Safety Coordinator who has received appropriate training that is relevant, regularly updated and meets the needs of the role.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to.

**Executive Headteacher & Senior Leaders**

The Executive Headteacher/Head of Academy has a duty of care for ensuring the safety (including Online safety) of members of the academy community, though the day-to-day responsibility for Online safety will be delegated to the Online Safety Co-ordinator. Any complaint about staff misuse must be referred to the Online safety Coordinator and the Designated Safeguarding Lead/ Deputy Safeguarding Lead, or in the case of a serious complaint, to the Executive Headteacher/Head of Academy.

**Executive Headteacher & Senior Leaders are responsible for:**

- Ensuring access to induction and training in Online safety practices for all users.
- Ensuring appropriate action is taken in all cases of misuse.
- Ensuring that Internet filtering methods are appropriate, effective and reasonable.
- Ensuring that staff or external providers who operate monitoring procedures be supervised
- Ensure that pupil or staff personal data as recorded within academy's management system sent over the Internet is secured.
- Ensure the ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly
- The Designated Safeguard Lead will receive monitoring update reports from the Online Safety Coordinator.

**Online safety Coordinator is responsible for:**

- Leading on Online safety meetings.
- Ensuring the ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Creating reports of Online safety incidents and creates a log of incidents to inform future Online safety developments,
- Reporting to the Education Team.
- Liaising with the Designated Safeguarding lead and/or the Safeguarding member of the Local Governing Committee & Executive Headteacher/Head of Academy to provide an annual report on Online safety.

**ICT Technicians:**

Under guidance from the Online safety Coordinator, the IT technician is responsible for ensuring:

- That the technical infrastructure is secure and is not open to misuse or malicious attack.
- That the academy meets required Online safety technical requirements and any relevant body Online safety Strategy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection strategy.

- The filtering strategy is applied and updated on a regular basis and 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Executive Headteacher/Head of Academy; Online safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

## 2. Communicating throughout the Academy

Rules relating to the code of conduct when online, and Online safety guidelines, are displayed around the academy and included within the staff handbook.
Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

## 3. Making use of ICT and the Internet

The Internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the academy's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils/students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave.

Some of the benefits of using ICT and the Internet are:

**For pupils:**

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- 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.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

**For staff:**

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

**For parents:**

- Ability to be involved in their child's learning through the use of our website and regular discussions with class teacher.

## 4. Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the academy as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright.

The academy will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites, then the URL will be reported to the Online safety coordinator. Any material found by members of the academy community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

## 5. Managing Information Systems

The academy is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of data and personal protection of our academy community very seriously. This means protecting the network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technicians/senior leaders will review the security of the academy information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the academy takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted i.e. encrypted USB and hard drives, via cloud sharing or through secure email services (the academy uses Egress).
- Making sure that unapproved software is not downloaded to any academy computers. Alerts will be set up and in use to warn users of this.
- Files held on the our network will be regularly checked for viruses.
- The use of user logins and passwords to access the network will be enforced.

For more information on data protection please refer to our Data Protection policy - available on request from the office. More information on protecting personal data can be found in section 11.

## 6. Emails

We use email internally this is an essential part of our communication. It is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally

Staff and pupils should be aware that the academy email accounts should only be used for academy-related matters, ie, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The Trust/academy has the right to monitor emails and their contents but will only do so if it feels there is reason to.

### 6.1 Email Accounts and Appropriate Use

The Russett school only permits email accounts in the academy that have been managed and approved by the academy. All staff are issued with an Academy email account and are required to check it at least daily for important communications.

When sending emails to third parties relating to pupils, any email that contains personal data or sensitive personal data (as defined by GDPR) must be sent using Egress (Secure email service). If an employee receives an email containing personal data or sensitive personal data relating to a pupil via an unsecured email service, they must report this to the Data Protection Officer.

**Staff should be aware of the following when using email in the academy:**

- Personal email accounts should not be used to contact pupils, parents or third party professionals and should not be accessed on school ICT equipment.

- Emails sent from academy accounts should be professionally and carefully written. Staff are representing the Trust/academy at all times and should take this into account when entering into any email communications.
- Staff must tell their line manager and/or the Safeguarding Lead/Executive Headteacher/Head of Academy if they receive any offensive, threatening or unsuitable emails either from within the academy or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in the academy.

**Students should be aware of the following when using email in the academy**, and will be taught to follow these guidelines through the curriculum and in any instance where email is being used within the curriculum or in class:

- Pupils should only use school-approved email accounts
- Excessive social emailing will be restricted
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the academy or from an external account. They should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Where appropriate, Pupils will be educated to identify spam and virus emails and attachments that could cause harm to the academy network or their personal account or wellbeing.

## 7. Published Content and the Russett School Website

The website is viewed as a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with the Trust/academy news and events, celebrating achievements and personal achievements, and promoting projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the academy community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the academy will be for the school office only. For information on the academy strategy on children's photographs and videos on the website please refer to section 7.1 of this strategy.

H Roberts holds responsibility for publishing and maintaining the content on our website, Facebook and Twitter page.
A weekly newsletter is written by the Head of Academy & Executive Headteacher. This is sent home by email and available on our website and Facebook for parents and carers.

### 7.1 Strategy and Guidance of Safe Use of Children's Photographs and Work

Colour photographs and pupils work brings our academy to life, showcase our student's talents, and add interest to publications both online and in print that represent the academy. However, we acknowledge the importance of having safety precautions in place to prevent the misuse of such material.

Under GDPR 2018, images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the academy parents/carers will be asked to sign appropriate consent forms. We ask this to prevent repeatedly asking parents for consent over the academic year. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the academy's strategy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- Academy strategy on the storage and deletion of photographs.

Records of consent are held on individual pupil files located in the office.

**Using photographs of individual children**

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have safeguards in place.

It is important that published images do not identify pupils/students or put them at risk of being identified. The academy is careful to ensure that images published on our website cannot be reused or manipulated. Only images created by or for the academy will be used in public and children may not be approached or photographed while in the academy or doing academy activities without the academy's permission. The academy follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all academy publications
  - on our website
  - in newspapers as allowed by the academy
  - in videos made by the academy or in class for projects.
- Electronic and paper images will be stored securely.

- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.

- Events recorded by family members of the students such as plays or sports days must be used for personal use only.

- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

- Any photographers that are commissioned by the academy will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school Safeguarding Policy.

### 7.2 Complaints of Misuses of Photographs and Videos

Parents should follow standard academy complaints procedure if they have a concern or complaint regarding the misuse of academy photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint.

### 7.3 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, vlogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These 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. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in the academy. There are various restrictions on the use of these sites that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The academy follows general rules on the use of social media and social networking sites:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of our code of conduct regarding the use of ICT and technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The Trust/academy expects all staff and pupils to remember that they are representing the Trust/academy at all times and must act appropriately.

- Safe and professional behaviour of staff online will be discussed at staff induction and regularly reinforced throughout the year.

### 7.4 Radicalisation and terrorism

The Prevent Duty requires all academy's to ensure that children are safe from terrorist and extremist material when accessing the internet in academies.
We have suitable filtering is in place through the use of: Smoothwall
Internet safety is an important part of our academy's Computing curriculum and also within PSHE and SRE.
General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website.

See our Child Protection & Safeguarding Policy for further information.

## 8. Mobile Phones and Personal Devices

While mobile phones, SMART watches and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying

- Can be used to access inappropriate internet material

- Can be a distraction in the classroom

- Are valuable items that could be stolen, damaged, or lost

- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The academy takes certain measures to protect pupils. Mobile phones are prohibited in the academy, this is detailed within our behaviour policy.

A member of staff will confiscate mobile phones, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device. The Trust/Academy accepts no liability for loss or damage to a device that has been confiscated.

Employees may use their own mobile device to access the following Trust-related resources: The Trust's Office 365 domain (including email, calendar, contacts, OneDrive, SharePoint, etc.), Arbor, other cloud-based systems. Permission for access using a personal device should be granted by The Head of Academy / Executive Headteacher, who will provide the requisite permissions. However where an employee is issued with a Trust device, this should be used in preference to a personal device.

In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the Trust networks. Passwords should not be shared or written down in line with our password protocols, as set out below.
The Trust's strong password requirement for personal devices is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols.

The device must lock itself with a password or PIN if it's idle for five minutes.

Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

Employees' access to Trust data is limited based on user profiles defined by IT and automatically enforced and as agreed by the Head of Academy / Executive Headteacher.

### 8.1 Mobile Phone or Personal Device Misuse including SMART watches

**Staff**

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of the academy.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the curriculum or for a professional capacity, the school equipment will be used for this.
- We expect staff to lead by example. The use of cameras on mobile phones, iPods/iPads (any device with picture or video taking facility) or the downloading of images onto any internet site is forbidden. Mobile phones should be stored away and are not permitted to be used in or around the academy.
- Any breach of the academy's strategy may result in disciplinary action against that member of staff.

## 9. Cyberbullying

The academy, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the Anti-bullying strategy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the academy 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 disciplinary action.

If an allegation of bullying arises, the academy will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine academy systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the academy will make sure that they understand what they have done and the impact of their actions
- Where digital self-harm is suspected, individuals or groups will be spoken to. It is important to give pupils time to discuss their actions and make sure that they understand their actions and consequence.

### 10. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The academy will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The academy keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

### 11. Protecting Personal Data

We believe that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-academy and individual progress. We collect personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

The Academy abides by the European General Data Protection Regulation (GDPR), which came into force on May 25 2018.

Refer to
Data Protection and Safeguarding policies.

### Equality Statement

On considering this policy there are no significat issues. Equality will always be reviewed as and when necessary or in the light of any changes.

In accordance with its Public Sector Equality Duty, the school has given due regard to equality considerations in adopting this policy/procedure and is satisfied that its application will not impact adversely on members of staff or pupils who have a protected characteristic (age, disability, gender, reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation, with the meaning of the Equality Act.

The Executive Headteacher will report on whether there have been any appeals or representations on an individual or collective basis on the grounds of alleged discrimination under any of the protected characteristics.