Rothersthorpe CE Primary School

E-safety Policy

September 2020

We are a happy, friendly and caring school that prides itself on being at the heart of our local community. We provide a unique environment that fully embraces our school family, village and church; a place where a range of people and groups gather in the pleasure of learning and growing together.

Each and every child is valued as an individual and helped to develop and progress in his or her unique way within a Christian environment. (Love your neighbour, as yourself. Mark 12:31)

Introduction

ICT and the internet have become integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media
- Mobile phones
- Laptops, tablets and ipads
- Online gaming
- Learning and communication platforms and Virtual Learning Environments
- Video broadcasting
- Blogs and Wikis
- Email, Instant Messaging and Chat Rooms

Why internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Scope of the Policy

This policy applies to all members of Rothersthorpe CE Primary School, (including staff, students / pupils, volunteers, parents / carers, visitors, community users), who have access to and are users of school ICT systems, both in school and off-site. It also applies to personal devices such as mobile phones and tablets belonging to pupils and staff brought onto school grounds

The Education and Inspections Act 2006 empowers Head teachers 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 school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by our School Behaviour Policy.

Rothersthorpe CE Primary School will deal with such incidents within this policy and associated behaviour, anti-bullying and safeguarding policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Rothersthorpe CE Primary School.

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

- meetings with the E-Safety Leader
- monitoring of e-safety incident logs
- monitoring of filtering
- reporting to relevant the Governing Body

Head teacher and Senior Leadership Team:

- The Head teacher has a duty of care for ensuring the safety, (including e-safety) of members of the school community.
- The Head teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Northamptonshire Local Authority disciplinary procedures).
- The Head teacher is responsible for ensuring suitable training is carried out as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Leader.

E-Safety Leader:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e- safety incident taking place.

- Provides training and advice for staff
- Liaises with the Local Authority / relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering
- Attends relevant meetings
- Reports regularly to Senior Leadership Team

Technical Support:

Technical Support Staff are responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required e-safety technical requirements and any Northamptonshire Local Authority E-Safety Policy that may apply
- Users may only access the networks and devices through secure passwords
- 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

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Rothersthorpe e-safety policy and practices
- They have read, understood and signed the staff Acceptable Use Policy
- They report any suspected misuse or problem to the Head teacher/E-Safety Leader for investigation
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems. However, if teachers are 'working from home' due to self- isolation or lockdown they are allowed to use their personal mobile device to call parents, (those who have parental responsibilities) for a consultation. The head teacher must be informed. However, teachers must ensure their personal number is blocked.

  How to temporarily block your number on any phone:

  Keying *67 or 141, before the phone number will block your caller ID on the call you're making. This works for both mobile and landline phones. Whoever you call will see 'private number', 'unavailable' or similar on their caller ID instead of the teacher's personal number. Once the call has been ended, the next call will display the teacher's caller ID as normal.
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use policies

- Pupils have a good understanding of research skills
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities, (where allowed), and implement current policies 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 any unsuitable material that is found in internet searches are dealt with using the Surf protect filtering system.

Child Protection / Safeguarding Designated Person
Should be trained in e-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

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Home School Agreement
- Have a good understanding of research skills
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying/
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Rothersthorpe E-Safety Policy covers their actions out of school.

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. Rothersthorpe CE Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / information about national or local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to the school social media accounts
- Their children's personal devices in the school, (where this is allowed) and whilst 'learning at home'

Policy Statements

Education – 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 e-safety is therefore an essential part of the school's e- safety provision. Children and young people need the help and support of the school to recognise and avoid e- safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and activities so that all pupils know the rules for safe internet use.
- Pupils will engage with an e-safety session led by a representative of an external organisation, e.g. the County e-safety officer or from the NSPCC, at least annually.
- Pupils should be taught in all lessons to be critically aware of the materials / content 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 helped to understand the need for the Home School Agreement and encouraged to adopt safe and responsible use both within and outside school
- 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 pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches are dealt with using the Surf protect filtering system.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. No filtering system can be 100% effective.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination), that would normally result in internet searches being blocked. In such a situation, staff can request that the Head teacher/E-Safety Leader, can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Breaches of filtering or access to inappropriate content by pupils must be reported to the e-safety coordinator and recorded on a Reporting log.

Education – Parents/Carers

Many parents and carers have only a limited understanding of e-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 school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Parents/Carers evenings / sessions
- High profile events / campaigns e.g Safer Internet Day
- Reference to the relevant web sites / publications *eg CEOP,* ThinkUKnow, Share Aware http://www.childnet.com/parents-and-carers (see school website for further lists of support)

Education – The Wider Community
Rothersthorpe CE Primary School will provide opportunities for members of the community to gain from the school's e- safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives, as well as parents
- The Rothersthorpe School website will provide e-safety information for the wider community

Education & Training – Staff / Volunteers
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An e-learning module and additional training from external providers as appropriate.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Staff Acceptable use policy (AUP).

Training – Governors
Governors should take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure / network 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 e- safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school technical systems and devices
- All users (at KS2) will be provided with a username. Users are responsible for the security of their username
- The administrator passwords for the school ICT system will be known and used with permission from the Head teacher
- The school bursar, is responsible for ensuring that software licence logs are accurate and that regular checks are made to reconcile the number of licences purchased against the number of software installations or full-time staff as appropriate.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband (Exa Education –Surfprotect and Stormshield)

Appropriate security measures are in place. Exa Education –Surfprotect and Stormshield is used 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 (Microsoft Security Essentials).

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 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 policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform 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.
- Photographs published on the school website, newsletters, school social media pages or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a school website or school social media pages, in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published around the school, on the school website, school social media pages, school newsletter or newspaper.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

General Data Protection Regulations

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

Rothersthorpe CE Primary School 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.
- It is registered as a Data Controller for the purposes of the General Data Protection Regulations (GDPR).
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear and understood routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear understandings about the use of cloud storage which ensure that such data 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 encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete

Communications

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

- Users must immediately report, to the e-safety coordinator and/or the Head teacher – in accordance with the school 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 pupils or parents / carers (email etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- If teachers are 'working from home' due to self- isolation or lockdown they are allowed to use their personal mobile device to call parents, (those who have parental responsibilities) for a consultation. The head teacher must be informed. Teachers must ensure their personal number is blocked.

  How to temporarily block your number on any phone:

  Keying *67 or 141, before the phone number will block your caller ID on the call you're making. This works for both mobile and landline phones. Whoever you call will see 'private number', 'unavailable' or similar on their caller ID instead of the teacher's personal number. Once the call has been ended, the next call will display the teacher's caller ID as normal.
- Pupils will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-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 website and only official email addresses should be used to identify members of staff.

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 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 school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school 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 school or local authority

Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- hate crimes
- radicalisation
- hacking
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures

Staff (and Volunteers) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

Rothersthorpe CE Primary School Acceptable Use Policy

This Acceptable Use Policy aims to ensure that:

- Staff and volunteers are responsible users and stay safe whilst using the internet and other communication technologies with regards to educational, personal and recreational use.

- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- Staff are protected from potential risk in their use of ICT in their everyday work.

- The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users. This policy should be read alongside the Staff Code of Conduct.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that Rothersthorpe CE Primary School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, ipads, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the E- safety Lead/Headteacher, Mrs Nicola Fountain.

I will be professional in my communications and actions when using Rothersthorpe CE Primary School ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Rothersthorpe CE Primary School:

- When I use my mobile devices (laptops, ipads, mobile phones, USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others to relevant members of staff. (Where digital personal data is transferred outside the secure local network, it must be encrypted.) Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems, (both in and out of school), and my own devices, (in school and when carrying out communications related to the school), within these guidelines.

Staff / Volunteer Name

Signed

Date

Appendix 1 - Reporting Log

E-Safety Reporting Log						
Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By		

Rothersthorpe CE Primary School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the Rothersthorpe CE Primary School network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's general data protection policy.
- logs are maintained of access to the internet by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Technician from EXA, our school Bursar, Carol Watt, Headteacher Nicola Fountain and E-Safety Governor Richard Parkin.

Technical Security

Policy statements

The school will be responsible for ensuring that the school network 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 will receive guidance and training and will be effective in carrying out their responsibilities

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as outlined in the e-safety policy.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems.

- The school infrastructure is protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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

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

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the General Data Protection Regulations. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". General Data Protection Regulation clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

Rothersthorpe CE Primary School recognises that data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

Updated September 2020