

E-Safety Policy including Acceptable Use

Rationale

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content for example: pornography, fake news, racism, misogyny, self-harm, suicide, radicalisation and extremism, online hoaxes or challenges.
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg relationships, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

E-Safety Policy

Our e-safety policy has been written by the school, following government guidelines. It has been agreed by all staff and approved by the governor's meetings and can be found on the school website.

Development, Monitoring and Review

This e-safety policy was approved by the governing body and the implementation of the e-safety policy will be monitored by the Computing Co-ordinator.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students/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 out of school, but is linked to membership of the school.

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

E-Safety Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the 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 governors on the Strategic Development Committee and the Safeguarding Governor and ICT Governor receiving regular information about e-safety incidents and monitoring reports.

Head Teacher:

- The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community. The day to day management for e-safety will be delegated to the e-Safety officers, as indicated below.
- The Head Teacher is responsible for ensuring that the e-Safety officers and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- 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.

e-Safety Officers

The day to day duty of the e-Safety Officers is devolved to Lisa Richmond, Sally Nicholson and Education Lincs. The e-Safety Officers will:

- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff
- Liaise with school's ICT technical staff- Education Lincs which is provided under contract
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments with an appropriate audit trail.
- Meet with the ICT governor to discuss current issues and review incident logs

- Attend relevant meetings
- Advise the Governing Body on all e-safety matters

ICT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical information is secure; this will include at a minimum:

- Anti-virus is fit for purpose, up to date and applied to all capable devices.
- Mac OS X (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as internet filtering are operating correctly
- Filtering levels are applied appropriately and according to the age of the user, that categories of use are discussed and agreed with the e-safety Officers and Head Teacher.
- Passwords are applied correctly to all users, regardless of age. It is recommended that passwords for staff be a minimum of 8 characters.
- Adherence to the Online Safety Act

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current e-safety policy and procedures
- They have read, understood and signed the school 'Staff Acceptable User Agreement'
- They report any suspected misuse or problem to the Head Teacher for investigation
- Digital communications with pupils (such as Google Classroom) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities - Use of Purple Mash scheme should ensure this is happening.
- Pupils follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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 processes are place for dealing with any unsuitable material that is found in internet searches. This is highly unlikely due to the school's filtering policy but any breach should be reported immediately to the Head Teacher.

Designated Safeguarding Leads:

The Designated Safeguarding Leads (DSLs) should be trained in e-safety issues and be aware of the potential for serious child protection 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 ICT systems in accordance with the 'Pupil Acceptable Use Policy', which they will be expected to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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 school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Digital leaders:

- Volunteer to undertake training and work alongside Computing Lead to deliver safety messages to their peers and parents via newsletters, Collective Acts of Worship and Learning Forums.

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 school will therefore take every available opportunity to help parents understand these issues through:

- parents' evenings, letters and the website.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Agreement when joining the school before any access can be granted to school ICT equipment or services.

Teaching and Learning

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

- The school internet access will be designed expressly for pupil's use including appropriate content filtering.
- Pupils will, in the main, be using Purple Mash to access the IT curriculum. This is a safe domain for children to work.
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the internet to research. Including the skills of knowledge location, retrieval and evaluation.
- As part of the new Computing (ICT) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital foot print and cyber-bullying.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning.

Purple Mash

Whole-school approach to computing also supports e-safety with built in lesson plans and resources for staff and children to access. Licence for this produce is reviewed annually.

Tapestry

Foundation Stage will use Tapestry as a means of communicating a child's progression in learning and next steps. Communication via Tapestry will be monitored by the Teacher and Business Manager and if any issues or concerns arise either party should contact the Head Teacher immediately.

Remote and Home Learning

Where necessary and in line with the school's policy/risk assessment, remote learning will be provided and/or delivered digitally. This may include but not limited to links to secure and reputable learning platforms, websites, application and digital worksheets. Where filmed elements are included, staff will strictly follow the current safeguarding and GDPR policies to ensure safety of all users and that communication between all parties concerned is recorded via official channels.

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses.

However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL, date, time and content shall be reported to the teacher who will then record the incident on the e-safety log which will be stored in the School Office. The e-safety log will be reviewed termly by the Computing coordinator.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work with its technical support provider (Education Lincs) to ensure filtering systems are effective as possible. We have in place web-filtering that blocks access to social media sites, chat rooms, online gaming sites and certain video hosting websites that do not have an internal filtering system.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety. This school:

- Education Lincs provides staff and governors with an email account (linked to a google for education account) for their professional use.
- Provides pupils with their own email (linked to a google for education account) supplied on request by Education Lincs.
- Pupil email is limited to only contact approved addresses and those with the @elstonallsaints domain.
- Does not publish personal email addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses for example, office@elstonallsaints.notts.sch.uk
- Will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary the Police.
- Knows that spam, phishing and virus attachments can make emails dangerous.
- Staff and governors are aware that emails are subject to Freedom of Information requests, and as such use email systems for professional purposes only.
- Staff and governors use a 'closed' email system which is used for LA communications and some 'LA approved transfers of information'
- Never use email to transfer staff or pupil personal data. We use secure, LA/DfE approved systems.

Social Networking

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites in the school is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

School staff will ensure that in private use:

- All staff are advised not to have contact with parents and children on any social networking site.
- No reference should be made in social media to students/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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Mobile Phones/Smart Watches

Many mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

Staff:

- Staff should not use mobile phones to contact parents/guardians. School Staff will always use the school phone to contact parents/guardians.
- The sending of abusive or inappropriate text message is forbidden.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or on the playground.
- Staff may use their mobile phones for personal use in the staffroom during the lunch period or before/after school.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Pupils:

- The school does not allow pupil mobile phones and tablets to be brought into school. Exceptions to this rule can only be sanctioned by the Head Teacher.
- Watches capable of recording sound or video may not be worn by children.
- If a pupil breaches the school policy, then the phone or device will be held in a secure place in the school office. These will then be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact their parents, they will be allowed to use the school phone.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

Parents/carers:

- Parents/carers cannot use mobile phones on school trips to take pictures of the children.
- Parents/carers are informed that at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

Visitors/Contractors

- Mobile phones may not be used by visitors or contractors when the children are on site.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- When using digital images, staff should inform and educate 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.
- Staff are allowed to take digital/video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment.
- Care should be taken when taking digital/video images that pupils are dressed appropriately and are not participating in activities that put them at risk or bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, 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 website, particularly in association with images.

- Permission from parents or carers will be obtained before photographs of pupils are published on the school website or any other platforms that the school uses.
- The Head Teacher or nominee will inform parents/carers and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email, telephone and fax numbers.
- Staff and pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure the content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website or any school platforms
- The governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- E-safety will be discussed with Education Lincs and those arrangements incorporated in our agreement with them.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Prevent Statement

The counter-terrorism and security bill was granted royal assent on 21 February 2015, which places a statutory duty on named organisations, including schools, to have due regard towards the need to prevent people being drawn into terrorism.

The most important part of this security bill is 'keeping pupils safe from the danger of radicalisation and extremism'.

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems used at All Saints Anglican Methodist Primary School block inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content they must report it to the e-Safety Officer or Head Teacher. Please refer to the Preventing Radicalisation Policy.

Cyber Bullying

- Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. All Saints Anglican Methodist Primary School have a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy. These include:
- No access to mobile phones nor public chat-rooms, Instant Messaging services on devices.

- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) may be given as part of an annual Anti-bullying Week and E-safety Events.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with their teachers.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our Anti-bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

Handling e-safety complaints:

- Complaints of internal internet misuse will be dealt with by the Head Teacher.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils and the E-safety Policy

- Rules for Internet access will be posted in all classrooms.
- Pupils will be informed that internet use will be monitored.
- Pupils will be informed when they are in KS2 of the importance of being safe on social networking sites. This will be strongly reinforced across all the year groups during computing lessons and all year groups look at different areas of safety through the digital learning lessons.

Staff and the e-safety policy:

- All staff will be given the school e-safety policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents and the E-safety Policy:

- Parent's attention will be drawn to the School e-safety policy on the school website.
- The parents will be encouraged to discuss code of conducts with their children before they are then asked to sign the 'Pupil Acceptable Use Agreement'.

Review

This policy will be reviewed annually.

Policy written October 2024

Review October 2025

Appendix 1 Acceptable Use – Staff and Governors

Note: All Internet and email activity is subject to monitoring - you must read this statement in conjunction with the above Policy.

USE OF E-MAIL AND INTERNET (including Social Media)

It is the responsibility of a school to ensure that all users use e-mail and Internet service in an acceptable manner and in accordance with the schools acceptable use policy and any e-mail and Internet agreements established by the school. Schools should use Nottinghamshire County Council's email and Internet code of practice for schools to establish their own policies on the acceptable use of email and internet.

The Internet provides users with access to worldwide information services, bringing new opportunities for communication. With the increasing popularity of social media tools such as Facebook and Twitter thought should be given when using these tools for publishing information about a school.

Social media tools are excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with users and the wider community.

Whilst social media tools can provide tremendous benefits to schools they also have serious security risks in their use. Risks such as people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and exploit children. In order to mitigate these security risks and still enjoy the benefits of social media schools should establish and enforce good social media usage policies which should include the following points:

- Supervision in the classroom with social media technology must be appropriate to the children's needs and abilities;
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school community should be aware that filtering software is not always effective and cannot always be relied on alone to safeguard children;
- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks;
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online;
- All pupils and staff should understand how to critically evaluate online content;
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the schools Leadership Team and Governors;
- ICT tools provided by the school should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than personally owned equipment.

Social networking – is allowed in school in accordance with this policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. It is acceptable for staff to 'like' and/or share school social media content but they are advised to refrain from comment. It is advised that staff members' personal accounts protect their privacy. Staff should not become 'friends' with pupils on personal social networks under any circumstances. Staff would not normally 'friend' parents except where there is an existing link outside the professional setting.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

PASSWORDS

The school is responsible for establishing and enforcing a password policy for its use of ICT. The Head Teacher is responsible for establishing and enforcing a password policy on their systems based on the level of security required. Passwords must be assigned to individual users of ICT systems to maintain security and the data that they contain.

Appropriate:

- Users only using their own account to carry out day to day work;
- Users not disclosing their password to allow others to access their account. Users should be aware passwords are for the benefit of the school and are the proprietary and confidential information of the school;
- Users selecting a password that is easy to remember but not for others to guess;
- Users not selecting obvious passwords, such as the name of a close relative, friend or pet;
- Compliance with the password policy for each computer system.

Inappropriate:

- Requesting passwords personally assigned to other users;
- Using a session via another user's password;
- Sharing passwords with other users. All users must take reasonable precautions to protect their passwords;
- If a user thinks that their username or password has been used without their permission, they must change the password and inform the head teacher as soon as practically possible. The head teacher will ensure that new users are issued with appropriate usernames and passwords. When a user leaves their job, whether leaving the school or not, the head teacher will ensure that all usernames and passwords for that user are suspended as appropriate.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen-drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Elston All Saints Anglican Methodist Primary School recognise that staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tables and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and suitable advice provided.

Appendix 2 – Own Device Usage Acceptance must be signed by all staff.

USE OF PCs, LAPTOPS & SERVERS

Appropriate:

- Storing school data;
- Loading text, images, video or audio streams in connection with day to day work activities;
- Storing limited amounts of personal data (where agreed by the head teacher).

Inappropriate:

- Loading unauthorised or untested software;
- Allowing unauthorised users to access laptops used away from school;
- Failure to keep laptops used away from school secure;
- Storing confidential or personal data or information on removable media without adequate protection or encryption;
- Deliberate, reckless or negligent introduction of viruses;
- Storing personal material protected by copyright which has not been purchased;
- Loading files containing pornographic offensive or obscene material.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Viruses and other malware - any virus outbreaks are to be reported to the Education Lincs Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

THE LEGAL FRAMEWORK

ICT use in a school setting should be legally regulated, this includes the content of e-mail, or sites downloaded from the Internet; privacy issues, monitoring of communications and surveillance at work and employment relations. Further legal advice should be sought, if appropriate, from Council's Children and Young People's Services HR or Legal Services.

If the school monitors e-mails or scans for profanity/inappropriate content, then users should be warned of this through policies.

Appendix 2 – Own Device Usage Acceptance

Staff and Governors - Acceptable Use of Personal Devices

Elston All Saints Anglican Methodist Primary School recognise that many staff and governors choose to access school information from their own devices.

Any member of staff or governor wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff and governors must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff and governors to ensure that their devices are compliant.

If any member of staff or governor uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and governors and suitable advice provided.

Own device usage agreement

I understand and accept that should I choose to access school data on any personal device that I use or own must have, and use, suitable encryption to secure the data.

Any unlawful access of data on such a device will be my responsibility. I will report any theft or loss to the School Business Manager or Head Teacher as soon as is practicable.

When exchanging, gifting, upgrading or selling the device I shall ensure that access to any school data is removed and data that relates to school is securely deleted.

Name:

Signed:

Dated:

KS2 Pupil Acceptable Use Agreement – e-Safety Rules

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and home learning.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace
- I will only use online materials with appropriate reference made to the source materials.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only email people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone numbers, send a photograph or video, or given any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carers has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.

I have read and understood these rules and agree to them.

Pupil Name:

Signature:

Parent/Carer Signature:

Appendix 4

Elston All Saints Anglican/Methodist Primary School

KS1 Pupil Acceptable Use Agreement – e-Safety Rules

THINK BEFORE YOU CLICK

 S	I will only use the Internet and email with an adult
 A	I will only click on icons and links when I know they are safe
 F	I will only send friendly and polite messages
 E	If I see something I don't like on screen, I will always tell an adult.

Name:

Child's Signature:

Parent/Carer Signature: