'A journey of a thousand sites begins with a single click.' Anon

Introduction

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience. It is the duty of the school to ensure that every child and young person in its care is safe. E-Safeguarding includes all aspects of technologies and electronic communications including tablets and mobile phones. The purpose of internet use in school is to help raise educational standards and promote pupil achievement. This policy highlights the need to educate children and young people about the benefits and risks of using new technology and provide safeguards and awareness for users to enable them to control their online experiences.

This policy has been developed to ensure that all stakeholders are working together to safeguard and promote the welfare of children. E-Safeguarding is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of E-Safeguarding at all times, to know the required procedures and to act on them. Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support E-Safe practices in school. Concerns related to child protection will be dealt with in accordance with the school's Safeguarding Policy and should be reported to the designated persons.

This policy is to be referenced alongside the behaviour, safeguarding, internet, data protection and anti-bullying policies.

Aims of the E-Safeguarding policy

- To set out the key principles expected of all members of the school community at Normanton All Saints CE (A) Infant School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Normanton All Saints CE (A) Infant School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Scope of the policy

- This policy applies to the whole school community including Normanton All Saints CE (A) Infant Schools' Senior Leadership Team, governing body, all staff employed directly or indirectly by the school and all pupils.
- Normanton All Saints CE (A) Infant Schools' senior leadership team and governing body will ensure that any relevant or new legislation that may impact upon the provision for E-Safeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students or 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 cyberbullying, or other E-Safeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate E-Safeguarding behaviour that takes place out of school.

Communication of the policy

- The Senior Leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school E-Safeguarding policy and the use of any new technology within school.
- The E-Safeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community.

- Any amendments will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An E-Safeguarding module will be included in the ICT curriculum covering and detailing the schools E-Safeguarding policy.
- An E-Safeguarding training programme will be established across the school to include a regular review of the E-Safeguarding policy.
- The key messages contained within the E-Safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed E-Safeguarding messages across the curriculum whenever the internet or related technologies are used
- The E-Safeguarding policy will be introduced to the pupils at the start of each school year
- E-Safeguarding posters will be prominently displayed around the school (See health and safety boards)

Roles & Responsibilities

We believe that E-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership team:

- The Headteacher is ultimately responsible for E-Safeguarding provision for all members of the school community, though the day-to-day responsibility for E-Safeguarding will be delegated to the E-Safeguarding coordinator.
- The Headteacher and Senior Leadership team are responsible for ensuring that the E-Safeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safeguarding roles and to train other colleagues when necessary.
- All staff are included in E-Safeguarding training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- All temporary staff and volunteers including students are made aware of the school's E-Safeguarding Policy and arrangements.
- A commitment to E-Safeguarding is an integral part of the safer recruitment and selection process of staff and volunteers.
- The Senior Leadership team will receive monitoring reports from the E-Safeguarding Coordinator.
- The Headteacher and Senior Leadership team should ensure that they are aware of procedures to be followed in the event of a serious E-Safeguarding incident.
- A senior member of staff is designated as the Senior Information Risk Officer (SIRO) to assess the risk of the use of different types of technology and information data sets that are owned by the school.

Responsibilities of the Governing body:

- To read, understand, contribute to and help promote the school's E-Safeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the E-Safeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its E-Safeguarding strategy

Responsibilities of the E-Safeguarding coordinator

- To promote an awareness and commitment to E-Safeguarding throughout the school
- To be the first point of contact in school on all E-Safeguarding matters
- To take day-to-day responsibility for E-Safeguarding within school and to have a leading role in establishing and reviewing the school E-Safeguarding policies and procedures
- To lead the school E-Safeguarding group or committee
- To have regular contact with other E-Safeguarding committees, e.g. the local authority, Local Safeguarding Children Board
- To communicate regularly with school technical staff
- To communicate regularly with the designated E-Safeguarding (Safeguarding) governor

- To communicate regularly with the senior leadership team
- To create and maintain E-Safeguarding policies and procedures
- To develop an understanding of current E-Safeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in E-Safeguarding issues
- To ensure that E-Safeguarding education is embedded across the curriculum
- To ensure that E-Safeguarding is promoted to parents and carers
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To monitor and report on E-Safeguarding issues to the E-Safeguarding group and the senior leadership team as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safeguarding incident
- To ensure that an E-Safeguarding incident log is kept up to date

Responsibilities of Teachers and Support staff:

- To read, understand and help promote the school's E-Safeguarding policies and guidance Also adhere to
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the E-Safeguarding coordinator
- To develop and maintain an awareness of current E-Safeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed E-Safeguarding messages in learning activities across all areas of the curriculum. To supervise and guide pupils carefully when engaged in learning activities involving technology
- To be aware of E-Safeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of pupils:

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To help and support the school in the creation of E-Safeguarding policies and practices and to adhere to any policies and practices the school creates
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices
- To know and understand school policies on the use of cameras and images
- To know and understand school policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss E-Safeguarding issues with family and friends in an open and honest way.

Responsibilities of parents

- To help and support the school in promoting E-Safeguarding
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To discuss E-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school it states 'I will ensure that any images or videos taken during school events are for my own personal use and will not be published on the internet including social networking sites e.g. Facebook' Parents and carers are asked to read through and sign alongside their child acceptable use agreements on behalf of their children on admission to school Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances. (Please see Appendix 1)

Staff training and professional development

- Our staff receive regular information and training on E-Safeguarding issues from the E-Safeguarding co-ordinator on a termly basis
- As part of the induction process all new staff receive information and guidance on the E-Safeguarding policy, the school's Acceptable Use Policies and the E-Safeguarding induction procedures
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate E-Safeguarding activities and awareness within their curriculum areas

Using images, video and sound

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done on entry to the school. This includes permissions for: website, press including newspapers, school displays (See consent form in Appendix 1) Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound.
- Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- The school will store images of pupils that have left the school for three years following their departure for use in school activities and promotional resources.
- Staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils. They must use the school's VPN access and store images centrally.
- The ICT technician has the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

Teaching and learning

E-Safeguarding and new technologies are an important part of the statutory National Curriculum. The internet benefits education by allowing access to world - wide educational resources. The school Internet access is designed expressly for pupil and educational use. All internet access shall be filtered for inappropriate images and websites in accordance with the local authority, Yorkshire and Humber Grid for Learning (YHGfL) and Internet Watch Foundation (IWF) policies. Children are taught what Internet use is acceptable and what is not through 'Sid's rules for using the internet' posters. Clearly planned learning objectives for using the Internet are shared with the children before the session and pupils are taught how to safely search for internet content of all types (images, information, video, music etc.) in order to further their learning. We provide a series of specific E-Safeguarding-related lessons in every year group as part of the ICT curriculum. (See long term planning) We will celebrate and promote E-Safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year. We will discuss, remind or raise relevant E-Safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use. Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas. Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way. We will remind pupils about their responsibilities through the school's Acceptable Use Policy which every pupil will sign. Staff will model safe and responsible behaviour in their own use of technology during lessons. We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content. Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. As a whole school pupils and staff have been educated on 'Hector the Protector' and the icon is available on every computer within school. Children are taught what to do if they access inappropriate material by clicking on the 'Hector' icon and waiting for a member of staff who will resolve the issue.

Managing ICT systems and access – *The school has an SLA in place with external ICT management company (MINT)*

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- ICT hardware and infrastructure will be located securely with only appropriate staff permitted access.
- ICT hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- At Key Stage 1, pupils will access the internet using a personalised log in, which the teacher supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

Managing passwords

- A secure and robust username and password convention exists for all system access (this includes a Capital letter and number combination including password length.) (email, network access, school management information system).
- Key Stage 1 pupils will have a personalised log on for all school ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- Users should be prompted to change their passwords at pre-arranged intervals or at any time that they feel their password may have been compromised.
- Users will change their passwords whenever there is any indication of possible system or password compromise

- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords e.g. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters including a number and where applicable a character.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure the password is.

Managing internet access

- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.
- Pupils will be taught what to do if they experience material that they find distressing, uncomfortable or threatening by clicking on 'Hector the protector' and referring to 'Sid's rules'

Managing email

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked (other email accounts must be approved by the Headteacher)
- Pupils will be allocated a whole class or group email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.
- Staff should not use personal email accounts for professional purposes, especially to exchange any school-related information or documents.
- Whole class or group email addresses will be used in school for communication outside of the school.
- Access, in school, to external personal email accounts may be blocked.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers, as approved by the senior leadership team and the Senior Information Risk Officer.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Email usage

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone as introduced by 'Hector the Protector'.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal email account.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Pupils and staff should never open attachments from an untrusted source but should consult the network manager first.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within school should report any inappropriate or offensive emails through the incident-reporting mechanism within school.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence. Teachers and admin staff should check their emails on a daily basis during working hours.

Managing school website content

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of pupils will not be used without the written consent of the pupil's parents/carers.
- The point of contact on the school website will be the school address and telephone number. Staff or pupil's home information will not be published.
- The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school's policy on image taking and publishing.
- Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused. The names of pupils will not be used on the website, particularly in association with any photographs.
- Work will only be used on the website with the permission of the pupil and their parents/carers.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Filtering

- The school uses a filtered internet service. The filtering system is provided by RM in line with the prevent duty.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils. The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-Safeguarding Coordinator. All incidents should be documented.

- If users discover a website with potentially illegal content, this should be reported immediately to the E-Safeguarding Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The school will regularly review the filtering product for its effectiveness. Any issues regarding filtering are brought immediately to the E-Safeguarding persons who will log incidents.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked. Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Social networking, social media and personal publishing

- All staff and governors receive a copy of the school's Social media policy and the Local Authorities Social Media policy in their induction packs

Mobile phones, hand held devices and Smart watches

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time (Unless permission has been granted by the Headteacher). They should be stored with personal belongings and preferably be on silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the express consent of the Headteacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and any photographs/video of children should be taken using school owned devices.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.
- Smart watches such as I-Watches can be worn for work by members of staff. They are to be disconnected from the mobile phone they are paired with during working hours either by disabling notifications or switching on airplane mode.

Protecting personal data

- The school adheres to the standards set out by the Data Protection Act 1998
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- Access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.

- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- Fax machines will be situated within controlled areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. remote access over encrypted tunnel (VPN) or encrypted removable media (hardrive),
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.
- For further information see the school's Data protection policy

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal
- Redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Dealing with complaints

- Staff, children and parents/carers must know to report incidents to the Headteacher. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- All E–Safeguarding complaints and incidents will be recorded by the school, including any actions taken
- The school's designated person for E-Safeguarding will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately. Any misuse will be logged electronically.
- Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

Sanctions for misuse for pupils may include any or all of the following:

- Discussion with the Headteacher
- Informing parents/carers
- Removal of internet access for a specified period of time

Parent and carers support

- Parents/carers will be informed of the school's E=Safeguarding policy which can be accessed via the school website.
- Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.
- Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.
- A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

- Parents/ carers will be expected to agree and sign the home/ school agreement which clearly states the use of photographic and video images outside of school.

Through all these measures we hope that children have a positive experience when using the internet and that ICT can be used as a tool to further development and teach vital life skills allowing children to make a positive contribution.

New and emergent technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safeguarding point of view. We will regularly amend the E-Safeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safeguarding risk.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable counter measures will be adopted within school to ensure that any risks are managed to an acceptable level.
- Emerging technologies can incorporate software and/or hardware products.
- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- All new technologies deployed within school will be documented within the E-Safeguarding and Acceptable Use Policies prior to any use by any member of staff or pupil.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school E-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed **Policy review**
- The school has an E-Safeguarding coordinator who will be responsible for document ownership, review and updates.
- The E-Safeguarding policy has been written by the school E-Safeguarding Coordinator and is current and appropriate for its intended audience and purpose.
- The school E-Safeguarding policy has been agreed by the senior leadership team and approved by governors.
- The E-Safeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The School has a member of the governing body who takes a lead responsibility for E-Safeguarding. All amendments to the school E-Safeguarding policy will be discussed in detail with all members of teaching staff.

Version control Title	Normanton All Saints CE (A) Infant E-Safeguarding policy
Version	6.0
Date	September 2017
Author	E-Safeguarding coordinator Danielle Edwards

Approved by head teacher
Approved by Governing Body
Next Review Date: September 2018