E-Safety policy

1. Mission Statement

Everyone at St John of Beverley RC Primary School knows we are part of God's family.
We share, play and learn together and try to be the best we can be.

2. Policy introduction

The purpose of this policy is:-

- To set out the key principles expected of all members of the school community at St John of Beverley RC Primary School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of St John of Beverley RC Primary 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.

3. Scope of policy

- This policy applies to the whole school community including St John of Beverley's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.
- St John of Beverley's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, 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 eSafeguarding-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 eSafeguarding behaviour that takes place out of school.

4. Review and ownership

- The school has appointed an eSafeguarding coordinator who will be responsible for document ownership, review and updates.
- The eSafeguarding policy has been written by the school eSafeguarding Coordinator and is current and appropriate for its intended audience and purpose.
- The school eSafeguarding policy has been agreed by the senior leadership team and

approved by governors.

- The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The School has appointed a member of the governing body to take lead responsibility for eSafeguarding.
- All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

5. Communication policy

- St John of Beverley's 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 eSafeguarding policy and the use of any new technology within school.
- The eSafeguarding policy will be provided to and discussed with all members of staff.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- An eSafeguarding or eSafety module will be included in the PSHE, Citizenship and/or ICT curricula covering and detailing amendments to the eSafeguarding policy.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used
- The eSafeguarding policy will be introduced to the pupils at the start of each school year

6. Roles and responsibilities

Responsibilities of the senior leadership team

- The headteacher is ultimately responsible for eSafeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator.
- The headteacher and senior leadership team are responsible for ensuring that the eSafeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

Responsibilities of the eSafeguarding Coordinator

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

- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that eSafeguarding education is embedded across the curriculum
- To ensure that eSafeguarding 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 eSafeguarding issues to the eSafeguarding 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 eSafeguarding incident

Responsibilities of teachers and support staff

- To read, understand and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the eSafeguarding coordinator
- To develop and maintain an awareness of current eSafeguarding 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 eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of eSafeguarding 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 technical staff

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system

- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted
- To be a member of the incident-management team that meets to review eSafeguarding incidents that have occurred within school

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 eSafeguarding 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 taking and use of mobile phones
- 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 be fully aware of research skills and of legal issues relating to electronic content such as copyright laws
- 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 eSafeguarding issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting eSafeguarding
- 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 eSafeguarding 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

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's eSafeguarding 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 eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy

Responsibilities of the Designated Safeguarding Lead

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to eSafeguarding and the safe use of technologies
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school

7. Managing digital content

7.1 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.

On the school website or blog

In the school prospectus and other printed promotional material, e.g. newspapers
In display material that may be used around the school
In display material that may be used off site

- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- 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. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, 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.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- 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.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

7.2 Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- Staff delegated by the Headteacher have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

8. Learning and teaching

- We will provide a series of specific eSafeguarding-related lessons in every year group/specific year groups as part of the ICT curriculum / PSHE curriculum / other lessons.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding 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 and the need to respect and acknowledge ownership of digital materials.
- 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 an end-user 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.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

Staff training

- Our staff receive regular information and training on eSafeguarding issues in the form of staff training.
- As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding 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 eSafeguarding activities and awareness within their curriculum areas

9. Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other 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 end-user 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 user ID and password, 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.
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- 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.

10. Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Key Stage 2 and above will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should 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.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
    - 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.

11. Emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- 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.
- The acceptable use of any new or emerging technologies in use within school will be

reflected within the school eSafeguarding 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.

12. Filtering internet access

- The school uses a filtered internet service.
- 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 by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding 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 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.

13. Internet access authorisations

- 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.
- When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.
- Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.
- Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

14. 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.
- Pupils will be allocated an individual email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.
- Staff and pupils are not permitted to access personal email accounts during school hours.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- 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.
- 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 and staff will be reminded about the dangers of revealing personal information within email conversations.
- Pupils must not reveal personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.
- 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 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.
- All pupils with active email accounts are expected to adhere to the generally accepted rules of netiquette; particularly in relation to the use of appropriate language. They should not reveal any personal details about themselves or others in email communication or arrange to meet anyone without specific permission.
- 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 pupils or staff access their school email (from home or within school), school policies still apply.
- Emails sent to external organisations should be written carefully and authorised before sending to protect the member of staff sending the email.
- 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 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.

15. Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

- Blogging, podcasting and other publishing of online content by pupils will take place within the school website.
- Any public blogs run by staff on behalf of the school will be hosted on the website and postings should be approved by the headteacher before publishing.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

16. Mobile phone usage in schools

General issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personal devices are not permitted to be used in certain areas including classrooms from the hours of 8.50-15.30.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned. In ‘emergency’ situations, any use must be declared to the DSL, the device will then be checked to ensure that images have been permanently erased.
- Pupil mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

Pupils’ use of personal devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers.

- If a pupil needs to contact his or her parents or carers, they will be allowed to use a 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 personal devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- 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.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the senior leadership team.
- 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, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

17. Data protection and information security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- 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.

- 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.

18. 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 data.
- All 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.

Policy Drafted by	Angela Nicholl
Adopted by the Governing Body	Feb 18
Date for Review	Feb 20