Saint Norbert's Catholic
Primary Voluntary Academy

E-Safeguarding Policy

(2018)

SAINT NORBERT'S CATHOLIC PRIMARY VOLUNTARY ACADEMY

E-SAFEGUARDING POLICY 2018

"To Live, Love and Learn in the Footprints of Jesus."

This policy outlines what our school considers acceptable use of the internet to mean. It is intended to provide a clear set of guiding principles for teachers, parents, governors, children and other stakeholders.

Safeguarding Children Statement

We fully recognise our responsibilities for safeguarding and promoting the health and well-being of all the children in our care. Our Designated Safeguarding representative for the school is Alex Dawson and the deputy designated representative for the school is Pam Tonge. The nominated Governor for Safeguarding is Freda Robinson.

UN Convention on the Rights of the Child

As a Rights Respecting School, we aim to ensure in particular, that:

- children enjoy the right to be educated
- children have the right to be treated fairly
- children have the right to be heard
- children have the right to be protected from exploitation
- children have the right to find things out and share this with others

Introduction

Computing skills and knowledge are vital to access life-long learning and employment; indeed ICT is seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All children and young people should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to children and young people and the professional work of staff, for example:

- access to world-wide educational resources
- access to experts in many fields
- educational and cultural exchanges between children and young people worldwide
- collaboration and communication within the wider context
- access to learning wherever and whenever convenient

The Internet enhances the management information and business administration systems for example within:

- communication systems
- improved access to technical support, including remote management of networks and automatic system updates
- online and real-time 'remote' training support
- secure data exchange between local and government bodies

Aims

- To set out the key principles underpinning the actions of all members of the school community at St Norbert's in relation to ICT-based technologies;
- To safeguard and protect children and staff at St Norbert's;
- 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.

This policy applies to the whole school community, including St Norbert's Senior Management Team, board of governors, all staff employed directly or indirectly by the school and pupils.

St Norbert's Senior Leadership Team and board of governors 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 cyber-bullying, 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 and 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.

Review and ownership

- The school has appointed an e-Safeguarding coordinator (Pam Tonge) 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 School has appointed a member of the governing body to take lead responsibility for E-Safeguarding.
- The E-Safeguarding Policy will be reviewed annually or when any significant changes occur.
- All amendments to the school E-Safeguarding Policy will be discussed in detail with all members of teaching staff.

Communication policy

- The St Norbert'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 E-Safeguarding Policy.
- The E-Safeguarding Policy will be formally 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.
- Staff CPD to include a regular review of the E-Safeguarding Policy.
- E-Safeguarding or E-Safety training will be part of the transition programme across the Key Stages and when moving between establishments, pupils responsibilities regarding the school E-Safeguarding Policy will be reviewed.
- Pertinent points from the school E-Safeguarding Policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.

- The key messages contained within the E-Safeguarding Policy will be reflected and consistent within all Acceptable Use Policies in place within school.

Roles and responsibilities

(Please see separate Social Media Policy for further information)

Responsibilities of the school community

We believe that E-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility in ensuring that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

Responsibilities of the Senior Leadership Team

- The Headteacher is ultimately responsible for E-Safeguarding provision (including E-Safeguarding) for all members of the school community, though the day-to-day responsibility for E-Safeguarding will be delegated to the E-Safeguarding Coordinator, Pam Tonge.
- The Headteacher and Senior Leadership Team (SLT) are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their E-Safeguarding roles and to train other colleagues when necessary.
- The Headteacher and Senior Leadership Team (SLT) will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal E-Safeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The Headteacher and Senior Leadership Team will ensure that they are aware of procedures to be followed in the event of a serious E-Safeguarding incident.

Responsibilities of the E-Safeguarding Coordinator

- Promote an awareness and commitment to E-Safeguarding throughout the school. Be the first point of contact in school on all E-Safeguarding matters.
- Take day-to-day responsibility for E-Safeguarding within school and have a leading role in establishing and reviewing the school E-Safeguarding policies and procedures.
- Provide a lead for the school's team of Cyber Mentors.
- Have regular contact with other E-Safeguarding committees, e.g. the local authority (LA), Local Safeguarding Children's Board (LSCB).
- Regular communication with school Network Manager, Ben Sass.
- Regular communication with the designated E-Safeguarding governor, Freda Robinson.
- Regular communication with the Senior Leadership Team (SLT)
- Create and maintain E-Safeguarding policies and procedures.
- Develop an understanding of current E-Safeguarding issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in E-Safeguarding issues.
- Ensure that E-Safeguarding education is embedded across the curriculum.
- Ensure that E-Safeguarding is promoted to parents and carers.
- Liaise with the local authority, the Local Safeguarding Children's Board (LSCB) and other relevant agencies as appropriate.
- Monitor and report on E-Safeguarding issues to the governing body as appropriate.

- Ensure all staff are aware of the procedures that need to be followed in the event of an E-Safeguarding incident.
- Ensure that E-Safeguarding incidents are logged.

Responsibilities of the E-Safeguarding Committee (Pam Tonge, Ben Sass, Freda Robinson and Alex Dawson)

- Ensure that the school E-Safeguarding Policy is current and pertinent.
- Ensure that the school E-Safeguarding Policy is reviewed at prearranged time intervals.
- Shall ensure that school Acceptable Use Policies (AUP) are appropriate for the intended audience.
- Promote, to all members of the school community, the safe use of the internet and any technologies deployed within school.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's E-Safeguarding policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
- Report any suspected misuse or problem to the E-Safeguarding coordinator.
- Develop and maintain an awareness of current E-Safeguarding issues and guidance.
- Model safe and responsible behaviours in personal use of technology.
- Ensure that any digital communications with pupils are on a professional level and only through school-based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- Embed E-Safeguarding messages in learning activities across all areas of the curriculum.
- Supervise and guide pupils carefully when engaged in learning activities involving technology.
- Ensure pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- Be aware of E-Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- Staff accessing school email on personal devices should sign a BYOD (Bring Your Own Device) policy.
- Understand and be aware of incident-reporting mechanisms that exist within the school.
- Maintain a professional level of conduct in personal use of technology at all times.

Responsibilities of Technical Staff - Network Manager, Ben Sass

(The school has signed a Service-Level Agreement with Ben Sass, who also has a current DBS certificate)

- Read, understand, contribute to and help promote the school's E-Safeguarding policies and guidance.
- Read, understand and adhere to the school staff AUP.
- Report any E-Safeguarding related issues to the E-Safeguarding coordinator.
- Develop and maintain an awareness of current E-Safeguarding issues, legislation and guidance relevant to work.
- Maintain a professional level of conduct in personal use of technology at all times.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Ensure that access to the school network only happens through an authorised and restricted mechanism.
- Ensure that provision exists for misuse detection and malicious attack.
- Take responsibility for the security of the school ICT system.
- Liaise with the Local Authority and others on technical issues.
- Document all technical procedures and review them for accuracy at appropriate intervals.
- Restrict all administrator level accounts accordingly.
- Ensure access controls exist to protect personal and sensitive information held on school-owned devices.
- Ensure appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.

- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Ensure controls and procedures exist so that access to school-owned software assets is restricted.
- Be a member of the incident-management team that meets termly to review E-Safeguarding incidents that have occurred within school.

Responsibilities of Pupils

- Read, understand and adhere to the school pupil Acceptable Use Policy (AUP).
- Know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- Know and understand school policies regarding behaviour.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- Take responsibility for own and 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 by pupils outside of school.
- Ensure that the feelings, rights, values and intellectual property of others are respected when using technology in school and at home.
- Understand what action should be taken if feeling worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home. Take similar action if aware of someone else who might be feeling the same.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and be fully aware of the incident-reporting mechanisms that exist within school.
- Discuss E-Safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safeguarding.
- Read, understand and promote the school's Acceptable Use Policy (AUP) with children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that children use in school and at home.
- Take responsibility for own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss E-Safeguarding concerns with children; show an interest in how they are using technology; and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in own use of technology.
- Consult with the school if there are any concerns about children's use of technology.
- Agree to and sign the Home-School Agreement.
- Read through and sign the pupil and parent Acceptable Use Agreements on behalf of children upon admission to school.

Responsibilities of the Governing Body

- Read, understand, contribute to and help promote the school's E-Safeguarding policies and guidance.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an understanding of how the school ICT infrastructure provides safe access to the internet.
- Develop an understanding of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the E-Safeguarding Committee 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.

- Ensure appropriate funding and resources are available for the school to implement its E-Safeguarding strategy.

Designated Safeguarding Lead, Alex Dawson

- Understand the issues surrounding the sharing of personal or sensitive information.
- Understand the dangers regarding access to inappropriate online contact with adults and strangers.
- Be aware of potential or actual incidents involving grooming of young children.
- Be aware of and understand cyber bullying and the use of social media for this purpose.
- Be aware of issues relating to the sending of indecent images or messages.

Other external groups

- The school will liaise with local organisations to establish a common approach to E-Safeguarding 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 (AUP) prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy (AUP) for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school.

Managing digital content

(Please see separate Social Media Policy for further information)

Using images, video and sound

Written permission from parents or carers will be obtained before photographs of pupils are published. This will be done annually or as part of the home-school agreement on entry to the school. This permission covers photographs or videos to be published:

On the school website or blog
On the school's learning platform
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
Via webcam in an educational conference

- 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.

- 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.

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.
- We will store images of pupils who have left the school – on school data storage facilities – for use in school activities and promotional resources, as appropriate and in accordance with our relevant GDPR policies.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- Each class teacher has the responsibility of deleting the images when they are no longer required, or as the school's Information Security and Confidentiality Policy dictates.

Learning and teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a series of specific E-Safeguarding-related lessons in every year group as part of the ICT curriculum / PSHE curriculum / other lessons. These will be particularly prominent in the Spring Term which coincides with E-Safety Day.
- 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 and wherever suitable opportunities arise during lessons. This will include the need to protect personal information; consider the consequences actions may have on others; the need to check the accuracy and validity of information used; and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be planned carefully 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.
- Pupils will be reminded about their responsibilities through signing the Acceptable Use Agreement.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Pupils will be taught how to search for information and to evaluate the content of websites that they use in any curriculum area for accuracy.
- 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.
- All pupils will be taught in an age-appropriate way about copyright (in relation to online resources) and understand about the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying.

- Pupils are 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, Cyber Mentors, Safe School Ambassadors, organisations such as Childline or the CEOP report abuse button.

Staff training

- Our staff receive regular information and training on E-Safeguarding issues in the form of In-Service Training.
- As part of the induction process, all new staff receive information and guidance on the E-Safeguarding Policy and the school's Acceptable Use Policies (AUP).
- All staff have been 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 are encouraged to incorporate E-Safeguarding activities and awareness within the curriculum areas for which they are responsible.

Managing the school E-Safeguarding messages

- 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.

Managing ICT systems and access

- The school will be responsible for ensuring that access to ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- 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.
- All pupils will be supervised while they have internet access within school.
- All users will sign an Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of and behaviour whilst using the school ICT systems, and that such activity will be monitored and checked.
- All internet access will be by working alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the school network – and therefore internet – using an individual username and password, which they will keep secure. Staff will ensure they log out after each session, and not allow pupils to access the internet through their username. They will abide by the school AUP at all times.
- When members of staff leave the school, there is an 'exit strategy' to remove all electronic access to school systems.

Passwords

- A secure and robust username and password convention exists for all system access (email, network access, school information management system).
- Key Stage 1 and 2 pupils will have a generic 'pupil' logon to all school ICT equipment.

- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged time intervals or at any such time 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 will 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 (AUP) prior to being given access to ICT systems, which clearly explains appropriate behaviour for protecting access to username and passwords.
- System passwords should not be written down.
- Personal passwords should only be disclosed to authorised ICT support staff when necessary, and never to anyone else. Stakeholders should ensure that personal passwords that have been disclosed are changed once the requirement is finished.
- Personal passwords should be used to access computer-based services, never shared with other users.
- Passwords should not be included in any automated logon procedures.
- System-based usernames and passwords should not be saved within an internet browser.
- All access to school information assets shall be controlled via username and password.
- No user should be able to access another user's files, without delegated permission being granted.
- Access to personal data is controlled securely in line with the school's Information Security and Confidentiality Policy.
- The school maintains a system log of all access by users and of their actions whilst using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Different passwords should be created for different accounts and applications.
- Passwords should feature numbers, letters and special characters (! @ # $ % * ( ) - + = , < > : : " '). The more randomly placed within the password, the better.

New technologies

(Please see separate Social Media Policy for further information)

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 use in school is allowed.
- All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure risks are reduced to an acceptable level.
- Emerging technologies can incorporate software and 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 should 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 should have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the E-Safeguarding Policy is adequate and that the implementation of the E-Safeguarding Policy is appropriate.
- 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 regularly.

Technology matrix

Communication technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school but only checked outside lesson times and kept out of view of pupils at all times		x						x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones or other camera devices except school camera or iPad				X				x
Use of handheld devices, e.g. tablets		x						x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of chat rooms / facilities other than DB Primary				x				x
Use of instant messaging				x				x
Use of social networking sites				x		x		
Use of blogs		x				x		

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 with regards the nature of content which can be viewed through the school's internet provision.
- The school has a clearly-defined procedure for reporting breaches of filtering (see Network Manager). All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy (AUP) and 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 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 this to appropriate agencies including the filtering provider, Local Authority, CEOP or Internet Watch Foundation (IWF).
- The school will regularly review the filtering product for effectiveness.
- The service provider will block all sites on the Internet Watch Foundation (IWF) list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed for content 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.

Internet access authorisations

- Parents will be asked to read and sign the school Acceptable Use Policy (AUP) for pupil access and discuss it with their child.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy (AUP) prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy (AUP) 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.
- 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.

Email

Account Management

- Staff and pupils should only use approved email accounts allocated to them by the school, and be aware that any use of the school email system will be monitored and checked.
- Pupils will be allocated an individual email account (DB Primary) for their use in school or class.
- Pupils may only use approved 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.

- Whole class or group email addresses will be used in school for communication outside of the school.
- Excessive social email use can interfere with learning and productivity and will be restricted in line with the school E-Safeguarding and Acceptable Use Policies.
- 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. School governors are provided with their own email addresses for the same reasons.
- 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 all school-related business.
- Staff will only use official school provided email accounts to communicate with pupils and parents and carers, as approved by the SLT.
- Under no circumstances should staff or governors contact pupils or 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.
- Stakeholders should never open attachments from untrusted sources; the network manager should be consulted 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 – and not reveal any personal details about themselves or others in email communication, nor 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 designated member of staff if they receive any inappropriate or offensive email.
- Stakeholders should remember that, irrespective of how they access school email (from home or within school), school policies still apply.
- To protect the sender, emails sent to external organisations should be written carefully and authorised before sending. All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) the Headteacher, line manager or another suitable member of staff into the email.
- Delete all emails that are no longer required or of any value.
- Check your email regularly for new email correspondence.
- Activate your 'out-of-office' notification when away for extended periods so colleagues are aware you are not currently available.

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

(Please see separate Social Media Policy for further information)

We use blogs/wikis/podcasts/social networking/other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform or school website and postings should be approved by the Headteacher before publishing.
- Pupils 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.
- Pupil photographs published on the school website will be anonymous to avoid identification.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- 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 of school.

Mobile phone usage in schools

Pupils' use of personal devices

- No pupil should bring his/her mobile phone or personally-owned device (including smart watches) into school unless prior permission is granted by the Headteacher.
- Any unauthorised device brought into school will be confiscated.

Staff use of personal devices

(Please see separate Social Media Policy for further information)

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people and 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.
- 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.
- Use of a mobile phone/text messaging in school should be restricted to emergencies only. Contact should be made using the office phone when calls are required during the school day.
- 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.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school-provided equipment for this purpose.
- 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 should 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.

Information Security and Confidentiality Policy

(Please see separate Social Media Policy for further information)

- 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 established an information-handing 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.
- All 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 no one else, who is unauthorised, can read the accessed information.
- All access to information systems should be controlled via a suitably complex password.
- All access to the school information management system will be on a need-to-know or least privilege basis.
- 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.
- 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. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.
- All devices taken offsite, e.g. laptops, tablets, removable media or phones will be secured in accordance with the school's information-handling procedures and not left in cars, for example.
- All school-owned hardware will be documented within a hardware inventory.
- All school-owned software will be documented within a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This should 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 over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We 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

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Policy updated: July 2018