St John's Priory School
Banbury

SAFEGUARDING CHILDREN
E- SAFETY POLICY
(INCLUSIVE OF CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA)

This policy applies to the whole school, including the EYFS

Legal status:
This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (2023), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Applies to:

- the whole school including the Early Years Foundation Stage (EYFS), the out of school care and extra-curricular activities inclusive of those outside of the normal school hours.
- all staff (teaching and support staff), the proprietors and volunteers working in, and those who supply services to, the School.
- both within and outside of normal school hours including activities away from school

Available from:

- This policy is publicly available on the school website or on request from the School Office

Monitoring and Review:

- This policy will be subject to continuous monitoring, refinement, and audit by the Headmistress
- The Online Safety Policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies.

Responsibility:
The Proprietors of the school are responsible for ensuring the implementation of procedures within this policy

M Jenkin

Michelle Jenkin: Headmistress
Date 16th February 2024

Giorgio Mystkowski: Proprietor
Date 16th February 2024

Review Date: January 2027

Related Policies:
Safeguarding Policies
Staff Code of Conduct
Acceptable Use Policies

INTRODUCTION:

Aims

Our aim is to have a robust whole school approach to online safety, ensuring that it is an ongoing and interrelated theme within our safeguarding provision and practice. We aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and visitors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school
- community in its use of technology, including mobile and smart technology ('mobile devices').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Purpose

The primary purpose of this Policy is to safeguard pupils and staff at St John's Priory School. It details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources.

In accordance with legislative requirements we have a whole school approach to online safety. Our key message to keep pupils and young people safe is to be promoted and should be applied to both online and offline behaviours. Within this policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding Children-Child Protection Policy.

This policy informs and supports a number of other School policies, including our staff and pupil Codes of conduct, Safeguarding Children-Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. There is particularly significance in regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns.

THE 4 KEY CATEGORIES OF RISK

Our approach to online safety is based on addressing the following categories of risk, which we know to be considerable and ever evolving:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

ROLES AND RESPONSIBILITIES

The Proprietors have overall responsibility for monitoring this policy and holding the Headmistress to account for its implementation.

The Headmistress is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school

The Designated Safeguarding Lead (DSL):

- will co-ordinate regular meetings/training with staff to discuss online safety
- takes lead responsibility for ensuring that staff understand this policy and that it is being implemented consistently

- throughout the school
- works with relevant parties, as necessary, to address any online safety issues or incidents
- manages all online safety issues and incidents in line with the school child protection policy
- ensures that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensures that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School behaviour policy
- updates and delivers staff training on online safety
- liaises with other agencies and/or external services if necessary
- provides reports on online safety in School to the Headmistress and/or Proprietors.
- ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

The ICT Service Supplier:

- will put in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety
- mechanisms are updated regularly
- conduct a full security check and monitoring the school's ICT systems on an agreed basis
- block access to potentially dangerous sites and, where possible, preventing the downloading of potentially
- dangerous files
- ensure that any online safety incidents are notified appropriately

All staff and volunteers:

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an understanding of this policy
- Implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet
- ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with
- appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and
- offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to notify a member of staff or the Headmistress of any concerns or queries regarding this policy. Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

ONLINE SAFETY IN ACTION

As a school, we will help our pupils know how to use the Internet responsibly and to understand that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
Endeavour to keep pupils safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.

- Ensure that pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- Ensure that staff, volunteers and the board will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Put into place rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact within our EYFS setting.
- Ensure our Acceptable Use Policy (AUP) is implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Through our supplier, ensure that monitoring procedures are transparent and updated as directed by regulations.
- Deal with allegations of misuse or known incidents appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Through our suppliers, ensure that an effective online safeguarding support systems are to be put in place, for example, filtering and monitoring controls, secure networks and virus protection to ensure that the School's technical infrastructure is secure and is not open to misuse or malicious attack.

USE OF IT SYSTEMS

Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT) before using any school ICT resource. In addition:

- All staff will receive annual update online safety training.
- All staff will read the 'Teaching Online Safety In School Guidance' to supporting school to teach their pupils how to stay safe online, within new and existing school subjects' (DfE, June 2023)
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems is be made by authorised password, which must not be made available to any other person.
- At all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices. Staff are advised to follow the "How do I stay secure on the Internet?" section in the Online safety FAQ document.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Every request to do so should be auditable with clear reasons for the need.
- The Internet can be used actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the School approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Staff must not communicate with pupils through electronic methods such as social networking sites, blogging, messaging apps or private email.

Misuse or Abuse of technology

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the Headmistress.
2. The Headmistress or the DSL should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
5. No pupil or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

TEACHING AND LEARNING

Internet use is part of the curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. Online safety is a focus in all areas of the curriculum and key online safety messages are reinforced regularly, teaching pupils about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Staff should be vigilant in lessons where pupils use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with School policy.

Staff will be provided with sufficient online safety training to protect pupils and themselves from online risks and to deal appropriately with online safety incidents when they occur. Ongoing staff development training includes training on online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements

The School's Internet access is designed to enhance and extend education. Pupils will be given clear guidelines for Internet use. Access levels reflect the curriculum requirements and age of pupils. Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is a part of teaching/learning in every subject.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

Key Stage 1: Pupils will be taught to:	**Key Stage 2**: Pupils will be taught to:
• Use technology safely and respectfully, keeping personal information private • Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies	• Use technology safely, respectfully and responsibly • Recognise acceptable and unacceptable behaviour • Identify a range of ways to report concerns about content and contact
By the end of Year 6, all pupils will know: • That people sometimes behave differently online, including by pretending to be someone they are not • That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous • The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them • How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met • How information and data is shared and used online • What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context) • How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know	

Pupils Use of IT Systems

All pupils must agree to the IT Acceptable Use Policy before accessing the school systems. Pupils at St Johns Priory have a clear understanding of what is expected of them is the same online as it is offline. Pupils will be given supervised access to our computing facilities and will be provided with access to filtered and monitored Internet and other services operating at the School.

The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of pupils. The School will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.

The School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (https://saferinternet.org.uk/)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

COMMUNICATING AND EDUCATING PARENTS/CARERS IN ONLINE SAFETY

Parents will be provided with a copy of the IT User Acceptance Policy, and parents will be asked to sign it, as well as pupils aged eight and older. St John's Priory School recognises the crucial role that parents play in the protection of their pupils with regards to online safety. The School organises awareness sessions for parents with regards to online safety, which looks at emerging technologies and the latest ways to safeguard children from inappropriate content. The School will also provide parents and carers with information through newsletters, website and the parent portals. Parents/carers are always welcome to discuss their concerns on online safety with the School and are encouraged to support the school in promoting good online safety practice.

PROTECTING PERSONAL DATA

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The School recognises that if required, data may need to be obtained by relevant parties such as the Police.

RADICALISATION AND THE USE OF SOCIAL MEDIA TO ENCOURAGE EXTREMISM

The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;
- Accessing likeminded people where they are not able to do this off-line, creating an online community;
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

St John's Priory School has a number of measures in place to help prevent the use of social media for this purpose:

- Website filtering and monitoring is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*
https://assets.publishing.service.gov.uk/media/5a7f64ac40f0b6230268f3a8/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

Reporting of Online safety Issues and concerns Including concerns regarding radicalisation

St John's Priory School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding online safety should be made to the Designated Safeguarding Lead (DSL), who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the DSL. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children-Child Protection Policy.

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting pupils from the risk of on-line radicalisation. St John's Priory School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of pupils and know where and how to refer pupils and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The School cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile devices with Internet access (e.g. smartphones) are not governed by the School's infrastructure and bypass any and all security and filtering and monitoring measures that are or could be deployed.
- We will audit ICT use to establish if the Online Safety Policy is sufficiently robust and that the implementation of the Online Safety Policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Designated Safeguarding Lead will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the School systems with the exception of filtered and monitored *Wi-Fi* access.
- St John's Priory School takes measures to ensure appropriate IT filtering and monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking" (KCSIE 2023).
- St John's Priory School recognises that pupils may choose to circumvent certain safety precautions by using devices over mobile networks. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/pupil training.

Internet Security and Filtering and Monitoring Systems

Through our service provider, our School has security systems in place to filter, monitor and secure the internet traffic on site. These systems are to keep everyone safe, from blocking inappropriate content, to protecting our ICT systems from cyber-attacks. The monitoring side plays an important part of the system, which helps us to identify ways to improve security, and to better protect those that use it. By default, the system blocks and flags all inappropriate websites, illegal or unsuitable content, including pornography. Use of these kinds of site is not allowed on site.

Personal Mobile Electronic Devices (Phones, Laptops, iPads and Tablets)

Pupils

Pupils at St John's Priory School are not permitted to have mobile devices in school without advance permission from the Headmistress. On the rare occasions that a parent requests this permission, mobile devices will be kept on site and stored by the Headmistress in her office between the beginning and end of the school day, apart from when being used under supervision for specifics teaching requirements (e.g. laptops used to support children with SEND). St John's Priory School is not responsible for any devices lost or damaged by pupils.

Staff

These following rules apply to all members of staff, contractors, visitors and volunteers, with the exception of the School's Marketing Manager and the Headmistress, who are both permitted to use mobile devices (both School owned and personal) for photography and social media purposes.

The School allows staff to bring in personal mobile devices for their own personal use. Personal devices, which enable access to the Internet via mobile data or a mobile network, must be locked with a security pin/face or fingerprint recognition so that in the event of a child coming across the device, they would be unable to access content or services. Devices must be turned onto silent mode during working hours and should be stored in a drawer or bag.

The use of personal mobile devices is prohibited during working hours, save for during designated breaks or non-teaching times. At no time may personal mobile devices be used in the presence of children and, as such, devices used during breaks / non-teaching time may only be used in the staffroom, in school office areas or in an empty classroom. Personal mobile devices must not be used in classrooms where children are present or in the play areas at any time.

EYFS

With the exception of mobile devices belonging to the School, which are used to upload content to the Tapestry portal, School 's secure shared networks or for social media purposes, no mobile devices are to be used in the EYFS setting during the teaching day. Once photos / videos recorded on a School device have been uploaded to the approved locations, they should be deleted from the device.

General

Under no circumstances must devices of any kind be taken into the pupil toilets (this includes any device with photographic or video capabilities).

Staff must ensure that there is no inappropriate or illegal content on their mobile devices. Should any member of staff become aware of inappropriate or non-essential use of a mobile device, this should be reported to a member of the SLT and may be subject to disciplinary action. Staff should remind parents regularly of school policy with regard to mobile phone use.

Failure to comply with these requirements will result in disciplinary action being taken in accordance with the School's Disciplinary Policy.

CYBERBULLYING

The use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else is known as Cyberbullying. Cyberbullying (along with all forms of bullying) will not be tolerated, and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (Safeguarding Children-Child Protection Policy).

There are many forms of cyberbullying. The NSPCC have published the following ways children can be affected by cyberbullying:

- **Messaging** - sending threatening or abusive text messages
- The creating and **sharing embarrassing images or videos**
- **Trolling** – the sending of menacing or upsetting messages on social networks, chat rooms or online games
- **Exclusion** - excluding children from online games, activities or friendship groups
- Online **shaming**
- Setting up **hate sites** or groups about a particular child
- Encouraging young people to **self-harm**
- Voting for or against someone in an **abusive poll**
- Creating **fake accounts, hijacking or stealing online identities** to embarrass a young person or cause trouble using their name
- Sending explicit messages, also known as **sexting**
- Pressuring children into **sending sexual images or engaging in sexual conversations**.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

ICT-Based Sexual Abuse

The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and storing indecent images of pupils is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven.

Adults should not use equipment belonging to the School to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils.

Adults should ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed.

Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Social Media / Gaming Grooming and Offline Abuse

Our staff needs to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Taking and Storing Images of Pupils Including Mobile Phones

St John's Priory School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere on the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc.

APPENDIX 1: EYFS ONLINE SAFETY, INTERNET AND ACCEPTABLE USE POLICY

This policy, which applies to the whole school inclusive of the Early Years Foundation Stage, is in support of the health and safety policy and the individual health and safety assessments. This policy is publicly available on the School's website. On request a copy may be obtained from the school's office

Aim

The Acceptable Use Policy (AUP) will aim to:

- Safeguard pupils and young people by promoting appropriate and acceptable use of information and communication technology (ICT).
- Outline the roles and responsibilities of all individuals who are to have access to and/or be users of work-related ICT systems.
- Ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Scope

The AUP will apply to all individuals who are to have access to and/or be users of work-related ICT systems. This will include pupils and young people, parents and carers, early years teachers and their coordinators, volunteers, pupils, committee members, visitors, contractors and community users. This list is not to be considered exhaustive. Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where known, off-site.

Roles and Responsibilities

Head of Early Years - has overall responsibility for ensuring online safety and will be considered an integral part of everyday safeguarding practice. The Head of Early Years will liaise with the Designated Safeguarding Lead who will monitor the practice of online safety within the EYFS. This will include ensuring:

- Early years teachers and the Head of Early Years will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- The AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be open and transparent.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection.

Designated Safeguarding Lead (DSL) - must be a senior member of the management team who is to have relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is to be available at all times, for example, a Designated Deputy. The designated person for safeguarding will be responsible for ensuring:

- Agreed policies and procedures are to be implemented in practice.
- All updates, issues and concerns are to be communicated to all ICT users.
- The importance of online safety in relation to safeguarding is to be understood by all ICT users.
- The training, learning and development requirements of early years teachers and their coordinators are to be monitored and additional training needs identified and provided for.
- An appropriate level of authorisation is to be given to ICT users.

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of pupils and young people will address online safety. A safe ICT learning environment is to be promoted and maintained.

Early Years teachers - will ensure:

- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- ICT equipment is to be checked before use and all relevant security systems judged to be operational.
- Awareness will be raised of any new or potential issues, and any risks which could be encountered as a result.
- Pupils and young people are to be supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
- Online safety information is to be presented to pupils and young people as appropriate for their age and stage of development.
- Pupils and young people will know how to recognize and report a concern.
- All relevant policies and procedures are to be adhered to at all times and training undertaken as is to be required.

Pupils - will be encouraged to:

- Be active, independent and responsible learners.
- Abide by the Acceptable Use Agreement as to be approved by peers, early years teachers and their co-ordinators, parents and carers.
- Tell a familiar adult about any access of inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent).

Acceptable use by early years teachers and their co-ordinators:

Early years teachers and their co-ordinators should be enabled to use work-based online technologies:

- To access age-appropriate resources for pupils and young people.
- For research and information purposes.
- For study support.

Use of images:

We will only use images of our pupils for the following purposes:

- Internal displays (including clips of moving images) on digital and conventional notice boards within the school premises,
- Communications with the school community (parents, pupils, staff), for example newsletters, Tapestry.
- Marketing the school both digitally by website, by prospectus [which includes an iPad app], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

Misuse by staff

Any allegation relating to an early years practitioner or manager having misused any ICT resource in an abusive, inappropriate or illegal manner, must be reported to the Designated Safeguarding Lead immediately. Should the allegation be made against the Designated Safeguarding Lead, the matter must be directed to the Headmistress. In the event of an allegation against the Headmistress, the matter should be raised with Giorgio Mystkowski, Proprietor.

Procedures are to be followed as appropriate, in line with the Staff Code of Conduct, this policy, Safeguarding Children-Child Protection Policies and/ or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

Acceptable use by pupils:

Pupils and young people will also be informed of the behaviours, which will be deemed unacceptable. This will allow pupils and young people to take some degree of responsibility for their own actions. Pupils will only be able to download a file under the direct supervision of a member of staff and it will be virus checked prior to being opened. The use of game-style activities and websites should be monitored by teachers to determine suitability.

Acceptable use by visitors, contractors and others:
All individuals who affect or come into contact with the Early Years setting are expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with pupils and young people. All guidelines in respect of acceptable use of technologies must be adhered to. The School reserves the right to ask any individual to leave the School at any time.

Links to other policies
Behaviour Policy
Safeguarding Children-Child Protection Policy
E-Safety Policy
Personal, Social, and Emotional Development
Health and Safety Policy.

APPENDIX 2 – PUPIL AND PARENT ACCEPTABLE USE POLICY

S — **Safe:** keep safe by being careful not to give out personal information – such as your full name, email address. Phone number., home address, photos or school name – to people you are chatting with online

M — **Meeting:** Meeting someone you have only been in touch with online can be dangerous. Only meet people if you have your parents' or carers' permission and even then, only when they can be present.

A — **Accepting:** Accepting emails, messages or invitations, or opening files, pictures or texts from people you don't know could lead to problems and they may contain viruses or nasty messages.

R — **Reliable:** Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

T — **Tell:** Tell your parent, carer or other trusted adult is somebody or something makes you feel uncomfortable or worried, or if someone you know is being bullied online.

<u>Pupil Acceptable Use Policy</u>

All pupils must follow the rules outlined in this policy when using school ICT resources and equipment, including all Internet, accessed from both in and outside of school, and on school provided or personal electronic devices. Breaking these conditions may lead to; confiscation of any electronic devices, close monitoring of the pupil's network activity, investigation of the pupil's past network activity, withdrawal of the pupil's access and, in some cases, permanent removal from the School and even criminal prosecution. Pupils are also expected to take care of school-issued electronic devices and any damage to them may result in fines to replace or fix damaged devices. Misuse of the Internet will be dealt with in accordance with the school's Behaviour and Discipline Policy and, where there is a safeguarding risk, the Safeguarding Children-Child Protection Policy. The school is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Pupils are responsible for backups of any other data held. Use of any information obtained via the network is at the pupil's own risk.

Pupil access to networked resources is a privilege, not a right. Pupils will be expected to use the resources for the educational purposes for which they are provided.

Pupils are expected to use the network systems in a responsible manner. It is not possible to compile a complete set of rules about what is, and what is not, acceptable; however, the above should be a guide and in cases of dispute the decision of the Head of School will be final.

Pupil agreement:

I agree to follow the school rules on the use of school network resources and mobile electronic devices. I will use the network and all mobile electronic devices in a responsible way and observe all of the conditions explained in both the Online safety Policy and this Acceptable Use Policy. I understand and accept the consequences of breaking these rules.

Print pupil name………

Pupil Signature…………………………………………………………………………….Date…………………………….

Parent/Carer agreement:

I understand that my child has agreed to accept the terms of the Online safety and Pupil AUP Policy and I confirm that I accept the terms of the agreement. If my child brings any personal electronic devices to school, I understand that the pupil is responsible for its safekeeping and appropriate usage while in transit to and from and on campus.

I have read and understood the Online safety Policy and agree to check any updates as the school provides them

Print Parent/Carer name……………………………………………………………………………………………..

Parent/Carer Signature……………………………………………………………… Date…………………………….

APPENDIX 3: ACCEPTABLE USE OF ICT (STAFF)

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are required to sign this code of conduct. Members of staff should consult the school's Online Safety Policy and ICT Acceptable Use Policy for further information and clarification. You must not use any ICT on-site until you have signed this Code of Conduct document and logged it with the School Business Manager.

- I will respect all ICT equipment/facilities at St John's Priory School and will report any faults that I find or any damage that I accidentally cause.
- I agree to abide by this policy in respect of any of my own ICT equipment or mobile devices that I bring on site. If any ICT device (personal or school-issued) is being used inappropriately or illegally on site (or inappropriately in the presence of pupils), the Headmistress may request that the device be monitored. Failure to comply with the monitoring could result in informing the appropriate authorities.
- I understand that no photographs of pupils may be taken with or stored on my personal electronic devices, including cameras, iPads, mobile phones, or personal computers.
- Photos of pupils should not be uploaded to personal social media accounts
- I am familiar with the school's Data Protection Policy, and I agree I am responsible for the security of all personal data in my possession. I agree that all personal data that relates to an identifiable person and is stored or carried by me on a removable memory device will be encrypted or contained within password-protected files to prevent unauthorised access.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others then I will immediately ask for these details to be changed.
- I agree that my use of St John's Priory School ICT equipment/facilities will be monitored and may be recorded at all times. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using St John's Priory School equipment/facilities. I understand that I may temporarily access-blocked websites, services and other online resources using only tools that are provided by St John's Priory School. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of St John's Priory School ICT equipment/facilities including the email and Internet system are for educational purposes, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on-site or using St John's Priory School equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not deliberately view, send, upload or download any material that is unsuitable for the school environment whilst I am in that environment or using any ICT equipment/facilities belonging to St John's Priory School. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the Online safety Officer or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents, I will help to improve online safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the Online safety Officer. I will not access any material that the Online safety Officer has rated as unsuitable.
- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using St John's Priory School equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold St John's Priory School responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with pupils through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the school email system may be used.

Signed:____ Date:_________________

APPENDIX 4 : TAKING AND STORING IMAGES OF PUPILS

Legal status:

This policy was prepared with reference to Ofsted advice on the use of mobile phones for the Early Years Foundation Stage (EYFS), the Department for Education's published guidance on the use of mobile phones and UK law governing the use of mobile phones while driving.

Applies to:

- The whole school including the Early Years Foundation Stage (EYFS), out of school care, the afterschool clubs, the holiday club and all other activities provided by the school, inclusive of those outside of the normal school hours.
- All staff (teaching and support staff), pupils on placement, the Proprietors and volunteers working in the school.

Guidance on use of mobile phones by teaching staff including those in the EYFS

There are mobile devices with access to Wi-Fi owned by the School for the specific education purposes.
There are digital cameras available for staff to use.

Early Years Portfolios

Photographs taken for the purpose of recording a child or group of pupils participating in activities or celebrating their achievements is an effective form of recording their progression in the Early Years Foundation Stage and other areas of the school. However, it is essential that photographs are taken and stored appropriately to safeguard the pupils in our care. When pupils join our school, we ask parents to sign consent for photographs and videos to be taken for such purposes.

Teachers are responsible for the storage of School cameras or mobile devices, which should be locked away securely when not in use. Images taken and stored on school cameras should be downloaded onto their school-issued computer and deleted from the cameras.

Staff are not to use their own equipment to take photos of pupils. Under no circumstances must cameras of any kind be taken into the toilets (this includes any device with photographic or video capabilities).

In the Early Years, photographs are sometimes distributed to members of key workers to record in pupils' profiles. Staff are not permitted to make extra copies of the photographs in any format.

Photographs are also taken at group events and activities and displayed around the classroom, School and in photograph albums for all the pupils to look back on and to talk about with their friends and teachers about the events that have happened in the EYFS. For this we need to have written parental permission for photo release that is requested upon enrolment. Every parent has the right to refuse this request, in which case the child must not be photographed by any member of staff, by a parent, or by any outsider without the express permission for that occasion of the parent with whom the EYFS has a contract.

Storage and review of images

Images of pupils are stored securely. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our website, when expired material is deleted.

St John's Priory School website and social media sites

Photographs and videos may only be uploaded to the school's website or social media sites with the approval of the Headmistress or Marketing Manager. Pupil's surnames are never used on our website or social media sites. When pupils join St John's Priory School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld such photographs/videos are not published of the individual child concerned. Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

External photographers

Professional photographs are taken throughout the year at School shows, by local media and approved school photography organisations. The School Business Manager ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of pupils from inappropriate use of images. Pupils are always properly supervised when professional photographers visit St John's Priory School. Where appropriate, parents/carers are given the opportunity to purchase copies of these photographs.

Appropriate use of a mobile phone during the school day (including social networking)

Mobile phones have a place on outings or in school buildings, which do not have access to a school landline. In these cases, they are often the only means of contact available and can be helpful in ensuring pupils are kept safe.

- If required to use a personal phone to call a parent/carer, staff should input 141 to ensure their own number is withheld.
- By arrangement with SLT, a member of staff's mobile phone may be designated as the means of communication for specific activities. The leader of the trip should ensure all participants (including parents, volunteers and partners) in the activity are aware of this Mobile Phone and Camera Policy.
- When leaving the school building with pupils (e.g. for sport, or on school trips), the mobile phones of all members of staff must be switched on and turned to loud to ensure that staff can be contacted by the School. Contact numbers for all members of staff accompanying the pupils must be provided to the School Office and a list of contact telephone numbers for the parents/carers of all pupils should be held by the leader of the off-site activity (although these must be kept confidential).

Staff and social media

- Staff must not post anything onto social media sites that could be construed to have any impact on the School's reputation. (We advise all our staff to carefully restrict their social media profiles to ensure they cannot be contacted by parents and pupils). We also staff not to accept friend requests from pupils past or present.
- We explain to staff that although they are able to accept friendship requests from friends who may also be parents of pupils at the school, staff must be aware of the potential issues this could cause.
- Staff must not post anything onto social networking sites that would offend any other member of staff or parent using the setting.

If any of the above points are found to have occurred, then the member of staff involved will face disciplinary action, which may result in dismissal.

The School has the right to confiscate and search any mobile electronic device (personal or School-issued) if it suspects that a pupil or staff member is in danger or has misused a device. This will be done in accordance with the School's policy on searching.

Images that we use in displays and on our website

The images that we use for displays and communications purposes never identify an individual pupil. Instead, they name the event, the term and year that the photograph was taken (for example, 'Sports Day, Summer Term 2016'). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a pupil.

Media coverage

We will always aim to notify parents in advance when we expect the press to attend an event in which our pupils are participating and will make every effort to ensure that images including pupils whose parents/carers have refused permission for such images of their pupils to be used are not used. We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the pupils of celebrities.

Staff induction

All new members of staff are given guidance on the School's policy on taking, using and storing images of pupils.

Use of mobile devices for volunteers and visitors

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils. If staff observe that visitors are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school. The exception to this would be at an organised event. Staff should remind parents regularly of school policy with regard to mobile phone use with the following statement when announcing events:

Parental use of mobile devices within the School

The growth of mobile technology and interconnectivity has implications for the safety of pupils, so in order to reflect the policy on safeguarding and child protection, it is essential parents do not use their mobile devices in the School, apart from circumstances as outlined below. Parents must ensure mobile devices are not on display (switched off or silent mode) while in the presence of pupils or in public areas of the school such as during meetings and school events.

The School records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

Other mobile technology

At St John's Priory School, we recognise the value of mobile technology within our curriculum. When accessing the school WiFi, staff and pupils must adhere to their ICT Acceptable Use Policy. Staff, pupils, volunteers and parents are responsible for their own mobile devices and the school is not responsible for theft, loss, or damage.

Driving and the law

The use of hand-held phones while driving, whether to make or receive a call, is prohibited. The only exception to this will be in the event of a genuine emergency call to 999 or 112, if it would be unsafe for the driver to stop. Hand-held mobile phones used with an earphone and microphone are covered under the ban, as they still require the user to hold the phone to press buttons or to read a message on the phone's screen.

The Proprietors and employees of the School will not require any employee to receive or make calls on a hand-held mobile phone while driving. Mobile phones must instead be directed to the message/voicemail service while driving.

The School will not assist in the payment of any fine levied against anyone using a hand-held mobile phone while driving on School business. Notification of any contravention of these requirements may be regarded as a disciplinary matter.

APPENDIX 5: ONLINE SAFETY FAQS

How will the policy be introduced to Pupils?

- Rules for Internet access will be posted in all rooms where computers are used
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use is included in the PSHEE programme covering both home and school use.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Pupils will be made aware of the acceptable use of technology and sign upon enrolment

How will ICT system security be maintained?

- The School ICT systems will be reviewed regularly with regard to security, fileting and monitoring.
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers.
- Files held on the school network will be regularly checked.
- All network system and administration passwords are to be recorded by the IT Service Supplier (Blue Planet) and kept in a secure place with regular updates.

How will staff be consulted and made aware of this policy?

- All new staff will be taken through the key parts of this policy as part of their induction, and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this online safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read and abide by the Staff Code of Conduct - prior to using school ICT equipment in the school
- Staff will use a child friendly safe search engine when accessing the web with pupils.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a member of the Senior Leadership Team.
- Complaints of Internet misuse will be dealt with by the Headmistress or DSL.
- Any complaint about staff misuse must be referred to the Headmistress.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children-Child Protection Policy and procedures.
- Parents and pupils will work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to relevant information via email, in newsletters and on the parent portal.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Parents will be invited to attend an online safety workshop.

How is the safe use of ICT and the Internet promoted?

St John's Priory School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. St John's Priory School has in place an Internet firewall, Internet content monitoring and filtering, antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and St John's Priory School will further promote safe use of ICT and the Internet by educating pupils and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Pupils complies with copyright law. St John's Priory School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHEE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferInternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

How does the Internet and use of ICT benefit education in our school?

- Pupils learn effective ways to use ICT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with LA and DfE.
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will pupils learn to evaluate Internet content?

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- If staff or Pupils discover unsuitable sites, the URL (address) and content must be reported to the teacher immediately.
- Staff and pupils should ensure that their use of Internet derived materials complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How is filtering and monitoring managed?

Having Internet access enables pupils to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. Through our service provider, all unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to pupils. In addition, usage of our network will be continuously monitored and attempts to access unsuitable sites will be flagged to the School. The service provider will tailor the filtering to suit the individual needs of the School and the age of pupils. Although this filtering uses the latest security technology, parents/carers should be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

We believe that the benefits to pupils having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents/carers of minors along with St John's Priory School share the responsibility for setting and conveying the standards that pupils should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide pupils towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

- The School will work in partnership with parents/carers, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, they must report it to the DSL immediately.
- The school will take every step to ensure that appropriate filtering and monitoring systems are in place to protect pupils from unsuitable material and the methods used will be reviewed regularly.
- Any material that the School believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are emerging technologies managed?

ICT in the 21st Century has an all-encompassing role within the lives of pupils and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by pupils may include:

- The Internet
- E-mail
- Instant messaging (Messenger, WhatsApp, etc.) often using simple web cams
- Social media
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Apps
- Gaming sites
- Music download sites
- Mobile devices with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'Internet ready'.
- Smart devices with e-mail, web functionality and productivity apps (e.g. Smart TVs)

How the School will respond to misuse of ICT by pupils

Step 1: Should it be considered that a child has deliberately misused ICT, the parent/carer will be contacted to discuss the issue. The child may be temporarily suspended from a particular activity.

Step 2: If there are to be further incidents of misuse, the child will be suspended from using the Internet or other relevant technology for an increased period of time. The parent/ carer will be invited to discuss the incident in more detail with the Headmistress or Deputy Head and the most appropriate course of action will be agreed.

Step 3: The sanctions for misuse may be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child be considered to be at risk of significant harm, the Safeguarding Children-Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the police or Local Children's Social Care.

In the event that a child should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

General Housekeeping:

The ICT equipment used by the School represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order.

The following will apply:

- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

Rules for pupils using School technology?

- Do not use ICT without permission.
- Food and drink must not be consumed near any computer equipment anywhere in the School.
- Do not move about the room while seated on a chair.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Faults should be promptly reported to the class teacher and pupils must not attempt to remedy them themself.
- Be aware of correct posture. Always ensure that the chair is at the optimum height and that you are sitting correctly at the workstation.
- At the end of a session, log off/shut down and put away equipment according to instructions.

What has research into cyberbullying found?

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyberbullying is done by pupils in the same class or year group and although it leaves no visible scars, cyberbullying of all types can be extremely destructive.

- Between a fifth and a quarter of pupils have been cyberbullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyberbullying.
- There is more cyberbullying outside school than in.
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyberbullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyberbullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyber-bullied tell no one about the bullying.

What is the impact on a child of ICT based sexual abuse?

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

How do I stay secure on the Internet?

- Do not type any personal details (including your name or email address) into a web site unless you are absolutely sure of the authenticity and trustworthiness of the associated company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the Headmistress.

Why is promoting safe use of ICT important?

St John’s Priory School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

Do we have to have a separate *Prevent* policy?

The Prevent duties can largely be implemented through schools’ existing safeguarding duties using, for example, current reporting lines and training processes. It is not a requirement to create a separate dedicated *Prevent* Policy. However, the Home Office statutory guidance introduces a new requirement that policies “set out clear protocols for ensuring that any visiting speakers – whether invited by staff or by pupils themselves – are suitable and appropriately supervised." This protocol can be a standalone document or be part of another policy or document.

What IT filtering and monitoring systems must we have?

Our filtering and monitoring systems are managed by our service provider and comply with the requirements as laid out by the DfE.