Online Safety Policy

This policy is applicable to the whole school including Boarding and Early Years Foundation Stage.

Information Sharing Category	Internal Use, All Staff
Policy Owner	DSL
Reviewers	DSL – Jack Snell Head Teacher– Deneal Smith Bursar – James Bell Chair of Governors – Andrew Johnson
Authorised by	Head Teacher
Date Published	11th October 2022

Review Log	
	Oct 22
Date of next review	October 2023

1. INTRODUCTION

1.1 The purpose of this Policy is to safeguard pupils and staff at St John's Beaumont. 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 and statutory guidance. There is a whole school approach to keeping pupils safe online and online safety is to be promoted by all staff and members of the school community. All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours including activities away from school.

1.2 There are defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy.

1.3 Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Child Protection & Safeguarding Policy.

1.4 The staff and pupil IT Acceptable Use Policies are central to the Online Safety Policy and should be consulted alongside this policy.

1.5 Online safety is part of the IT curriculum, staff training, and also through parental engagement.

1.6 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.

1.7 The Pupil Parliament will be consulted regarding any changes to the IT Acceptable Use Policy for Pupils. All staff should read these policies in conjunction with the Online Safety Policy.

1.8 Online safety is an important part of the Prevent Strategy, as a large portion of cases of radicalisation happen online. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Child Protection & Safeguarding Policy.

2. MONITORING AND REVIEW OF THE POLICY

2.1 This policy is subject to continuous monitoring, refinement and audit by the Head Teacher and the Designated Safeguarding Lead (DSL). The Governing Council will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing.

2.2 All staff will be informed of the updated/reviewed policy and it is made available to them in either a hard copy or electronically.

3. ROLES AND RESPONSIBILITIES

3.1 Our nominated Online Safety Officer is Jack Snell (DSL) who, along with the members of the safeguarding team, has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice.

3.2 In collaboration with the on-site IT Support service of CST Ltd., the Online Safety Officer and Designated Safeguarding Team have the responsibility of ensuring:

- Pupils know how to use the Internet and connected devices responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- Pupils are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- Pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and child to child risks when using ICT, including cyberbullying and other forms of abuse.
- Pupils, staff, the Governing Council and volunteers will receive the appropriate Online Safety 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 Pre-Prep, Middle School and Upper School and Boarding settings. Such policies and procedures are to include the personal use of work-related resources.
- The IT Acceptable Use Policy 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 transparent and updated as agreed in school policies. Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with the Behaviour and Discipline Policy, Staff Behaviour Policy, Low Level Concerns Policy, and Child Protection and Safeguarding Policy 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 to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- 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.

- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- A current record of all staff and Pupils who are granted access to school ICT system is maintained.

3.3 Designated Safeguarding Lead (DSL): must have relevant, current and practical knowledge and understanding of child protection and safeguarding and online safety. The DSL and DDSLs 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 staff are to be monitored and additional training needs identified and provided for boarding specific training
- an appropriate level of access authorisation is given to ICT users.
- the curriculum addresses online safety.
- a safe ICT learning environment is to be promoted and maintained.

3.4 The Governing Council's responsibilities: provide pupils with a safe environment in which to learn and be safeguarded online. The Governing Council will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. As part of this process, the Governing Council has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the senior leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

3.5 All Staff: must be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of St John's Beaumont, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current Online Safety issues, and this online Safety Policy. Cyber-bullying incidents will be reported in accordance with school's Anti-Bullying Policy. All staff will ensure they understand and adhere to our staff IT Acceptable Use Policy, which they must sign and return to Safeguarding Team. Teachers will ensure they are confident in delivering the school's computing and Online Safety curriculum as required, identifying risks and reporting concerns as they arise.

3.6 Parents: are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. St John's Beaumont will support parents by sharing information and links through newsletters, the school website, social media platforms and informal/formal training. They will read the pupils IT Acceptable Use Policy ensuring their son understands full their responsibility as part of this policy.

3.7 All Pupils: will ensure they understand and adhere to our Pupil IT Acceptable Use Policy, which they must sign and return to the Safeguarding Team. Pupils are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

4. ONLINE SAFETY ISSUES

4.1 Breadth of Online Safety Issues: online safety issues can be classified into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams. These issues are to be managed by reducing availability, restricting access, promoting safe and responsible use.

4.2 Staff/Volunteers 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 IT Acceptable Use Policy before using any school ICT resource. In addition:

- All staff including the Governing Council will receive appropriate Online Safety training, which is updated regularly through staff inset.Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times staff must 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.

- 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. Student internet usage is also monitored through Impero which monitors blocked search terms and websites.
- 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 to 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 should not communicate with pupils through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e., videos of lessons, activities or fieldtrips, must be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.
- In order to strengthen the schools' defences against future cyber incidents, staff are encouraged to enable the Authenticator App for Office 365.

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

- Report in confidence to the school's Online Safety Officer/DSL.
- The Online Safety Officer should investigate the incident.
- If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of the staff or pupil IT Acceptable Use Policy, appropriate sanctions will be enforced.
- 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.
- 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.

5. TEACHING ABOUT ONLINE SAFETY

5.1. The school's internet access is designed to enhance and extend education. Pupils will be taught what internet use is acceptable and what is not and given clear guidelines for internet use according to the Pupil IT Acceptable Use Policy.

5.2 Access levels reflect the curriculum requirements and age of pupils.

5.3 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.

5.4 Staff should be vigilant in lessons where pupils use the internet by running Impero each time devices are used in lessons.

5.5 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.

5.6 The frequency, level and focus of such training will depend on individual roles and requirements. Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

5.7 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.

5.8 Access levels to ICT 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. This teaching is built into existing lessons alongside our wider whole-school approach.

5.9 Pupils will explicitly be taught the following topics through their lessons:

- What internet use is acceptable and what is not and given clear guidelines for internet use
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications
- How to evaluate what they see online
- How to recognise and respond to harmful online challenges and online hoaxes.
- How to recognise techniques used for persuasion
- Online behaviour

- How to identify online risks
- How and when to seek support.

6. CHILD-ON-CHILD ABUSE

6.1 St John's Beaumont recognises that child-on-child abuse can occur online and to this end we teach pupils how to spot early warning signs of potential abuse, and what to do if pupils are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- access to illegal, harmful or inappropriate images
- cyber bullying
- access to, or loss of, personal information
- access to unsuitable online videos or games
- loss of personal images
- inappropriate communication with others
- illegal downloading of files
- exposure to explicit or harmful content, e.g., involving radicalisation
- plagiarism and copyright infringement
- sharing the personal information of others without the individual's consent or knowledge.

7. HARMFUL ONLINE CHALLENGES AND ONLINE HOAXES

Please refer to the latest DfE Guidance: https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

7.1 There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach pupils to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

7.2 A case-by-case assessment, establishing the scale and nature of the possible risk to our pupils will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw pupils' attention to a potential risk.

7.3 The DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

8. PUPILS' USE OF IT SYSTEMS

8.1 All pupils must agree to the Pupil IT Acceptable Use Policy before accessing the school systems. Pupils at St John's Beaumont will be given supervised access to computing facilities and will be provided with access to filtered Internet and other services operating at the school (Pupil internet usage is monitored through Impero which monitors blocked search terms and websites.).

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

8.3 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.

8.4 Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-schools

- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

9. HOW IS THE CONTENT FILTERED?

9.1 Having Internet access enables students 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. All unsuitable websites will be filtered and automatically blocked by our security systems (Sophos Web & Firewall / Impero) and will not be made accessible to students. In addition, students' usage of our network will be monitored continuously and repeated attempts to access unsuitable sites will alert our IT Department and DSL Team. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of students. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

9.2 However, at St John's, we believe that the benefits to students 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 and guardians of minors along with St John's share the responsibility for setting and conveying the standards that students should follow when accessing and using the media information sources at school and/or at home. During school time, teachers will guide students 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.

9.3 Steps for managing filtering are:

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, they must report it to the ICT Coordinator immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect students 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 (https://www.iwf.org.uk).

10. EDUCATING STAFF

10.1 Online safety training opportunities will be available regularly to staff members (including the Governing Council) and content will include training on specific safeguarding issues, cyber bullying and radicalisation.

10.2 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.

10.3 The frequency, level and focus of such training will depend on individual roles and requirements.

10.4 Staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of Online Safety, as well as current developments in social media and the internet as a whole.

10.5 Staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

10.6 Any new staff members are required to undergo online safety training as part of their induction program, ensuring they fully understand this online safety policy, the social media policy and staff and pupil IT Acceptable Use Policy.

11. COMMUNICATING AND EDUCATING PARENTS/GUARDIANS IN ONLINE SAFETY

11.1 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 seven and older. St John's Beaumont recognises the crucial role that parents play in the protection of their children with regards to online safety. The school organises an annual awareness session for parents with regards to Online Safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents and carers with information through newsletters, web site and the parent portals. Parents and guardians are always welcome to discuss their concerns on Online Safety with the school, who can direct them to the support of our Online Safety Officer if required. Parents and carers will be encouraged to support the school in promoting good Online Safety practice.

12. PROTECTING PERSONAL DATA

12.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Pupils are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will act responsible for ensuring we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

13. RADICALISATION AND THE USE OF SOCIAL MEDIA TO ENCOURAGE EXTREMISM

13.1 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.

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

- Web site filtering is in place on the school network to help prevent access to terrorist and extremist material and social networking sites such as TikTok, SnapChat, Facebook, Instagram, 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.

13.3 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.'

14. REPORTING OF ONLINE SAFETY ISSUES AND CONCERNS INCLUDING CONCERNS REGARDING RADICALISATION

14.1 St John's Beaumont 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 Online Safety Officer 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 Online Safety officer. Complaints of a child protection nature must be dealt with in accordance with our Child Protection & Safeguarding Policy.

14.2 The Designated Safeguarding Lead provides advice and support to other members of staff on protecting pupils from the risk of online radicalisation. The school ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism.

14.3 The school ensures 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.

14.4 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.

15. 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 phones with Internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- The school carries out an annual audit of our Online Safety provision in October 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 Heads of School/Boarding 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 Wi-Fi access.
- The school takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- The school recognises that pupils may choose to circumvent certain safety precautions by using devices over 3G, 4G and 5G. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/student training.

16. MOBILE ELECTRONIC DEVICES

16.1 Day School:

- Mobile phones are not permitted in the day school for pupils, or during regular school activities e.g. during home or away sports fixtures.
- If a device is brought to school, St John's Beaumont is not responsible for any devices lost by pupils.
- Recordings or live streaming made using mobile electronic devices (e.g. photograph / film / audio recording) is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied
- School devices may be used by teachers where there are children present, but any images captured must be erased from the device if a teacher leaves the school site with this device, unless this is for the purposes of an educational school trip.
- Pupils' mobile phones will be confiscated if found and returned only at the end of the school day.

16.2 Staff Personal Devices:

- Staff must not use personal mobile phones in the presence of pupils.
- Staff must not use personal mobile phones to take photographs, film or record pupils in any way.

16.3 EYFS Setting

- No personal mobile phones are to be used in the Early Years setting during the teaching day.
- All members of staff working in EYFS will not use or carry personal mobile phones while working.
- Staff may use their phones during break and lunchtimes in the staffroom only. Designated school devices may be used to take photos and record information of the children's learning.

16.4 Boarding

- Mobile telephones and laptops are permitted in both boarding houses on Tuesday and Thursday during 7 – 7:25pm for Years 3 to 7 pupils and 8:15 – 8:45pm for the year 8 pupils.
- Recordings or live streaming made using mobile electronic devices (e.g. photograph / film / audio recording) is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.
- All electronic devices are welcome to be joined to the school network, school devices must be connected at all times to ensure proper filtering, and monitoring is taking place.

16.5 School trips

- The trip leader has discretion to allow the use of mobile phones during longer overnight school trips to allow for some contact with parents / carers.
- Teachers will be responsible for storing mobile phones and devices when not in use.
- As above, recordings or live streaming made using mobile electronic devices (e.g. photograph / film / audio recording) is prohibited during times when pupils are allowed access to their phones.

17. CYBER-BULLYING

17.1 Cyber-Bullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. 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 (see our Safeguarding & Child Protection Policy). Seven categories of cyber-bullying have been identified:

a) Text message bullying involves sending unwelcome texts that are threatening or cause discomfort;

b) Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;

c) Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;

d) Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;

e) Chat room bullying and online grooming involve sending menacing or upsetting responses to pupils or young people when they are in a web-based chat room;

f) Bullying through instant messaging (IM) is an Internet-based form of bullying where pupils and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, Google Hangouts etc.) as they conduct real-time conversations online;

g) Bullying via websites and social networks (an example of this would be TikTok, SnapChat, Facebook, Twitter, Instagram, etc.) includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

17.2. 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.

18. ONLINE SEXUAL HARASSMENT

18.1 Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

18.2 Online sexual harassment includes:

- non-consensual sharing of nude or semi-nude images and videos and sharing sexual images and videos (both often referred to as sexting);
- inappropriate sexual comments on social media;
- exploitation;
- coercion and threats.

18.3 Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence.

18.4 All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under the school's Child Protection and Safeguarding Policy.

18.5 Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g., for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated.

18.6 The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772, and helpline@saferinternet.org.uk, providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.

18.7 If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

19. SOCIAL MEDIA, INCLUDING TIKTOK, SNAPCHAT, FACEBOOK, TWITTER AND INSTAGRAM

19.1 TikTok, SnapChat, Facebook, Twitter, Instagram and other forms of social media are becoming an increasingly important part of our daily lives. Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

19.2 Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Head Teacher for reasons of work. Staff and pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others. Staff and pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever. Staff and pupils are aware that their online behaviour should at all times be compatible with UK law.

20. ICT-BASED SEXUAL ABUSE

20.1 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 are 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.

20.2 Pupils are reminded that sending nude or semi-nude images is strictly prohibited by the school and may constitute a criminal offence. Often referred to as 'sexting, the school will treat incidences of both sending and receiving these images as a safeguarding and/or child protection issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

20.3 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.

21. CHAT ROOM GROOMING AND OFFLINE ABUSE

21.1 Staff need 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.

22. COMMUNICATING AND EDUCATING PARENTS/CARERS IN ONLINE SAFETY

22.1 It is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. The school regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents will be provided with a copy of the Pupil IT Acceptable Use Policy, and parents of pupils from the Early Years to Year 3 will be asked to sign it on their child's behalf.

22.2 St John's Beaumont recognises the crucial role that parents play in the protection of their children with regards to Online Safety. The school organises annually awareness sessions for parents with regards to Online Safety, which look 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; Parents/Carers sessions. Parents and carers are always welcome to discuss their concerns on Online Safety with the school. Parents and carers are encouraged to support the school in promoting good Online Safety practice.

- Parents/carers are required to decide whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents/carers are expected to sign an agreement containing the following statement or similar:

  We will support the school approach to online safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school's name into disrepute.

22.3 The school disseminates information to parents relating to Online Safety where appropriate in the form of; posters and school website

23. TAKING AND STORING IMAGES OF PUPILS INCLUDING MOBILE PHONES

23.1 St John's Beaumont 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.

23.2 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.

24. REMOTE LEARNING

24.1 Where there are periods in which the school is forced to close yet continue to provide education (such as during significant rising respiratory infection rates, such as the Covid19 pandemic) it is important that St John's Beaumont supports staff, pupils and parents to access learning safely, especially considering the safety of our vulnerable pupils. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection & Safeguarding Policy and where appropriate referrals should still be made to children's social care and as required, the police.

24.2 Online teaching should follow the same principles as set out in the school's Staff Behaviour Policy and Behaviour and Discipline Policy.

24.3 The school will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

24.4 The school will put additional measures in place to support parents and pupils who are learning from home. This will include specific guidance on which programmes the school is expecting pupils to use and how to access these alongside how pupils and parents can report any concerns that they may have. Guidance will also be issued on which staff members pupils will have contact with and how this will happen, including how to conduct virtual lessons (including video calls).

25. RELATED DOCUMENTS

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy;
- Behaviour and Discipline Policy.
- PSHE & RSE Policy

26. LEGAL STATUS

This policy has regard to the following guidance:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, and amendments to these .
- Keeping Pupils Safe in Education (KCSIE) Information for all schools and colleges (DfE, 2022)
- Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.
- Working Together to Safeguard children (WT) (2018) which also refers to non-statutory advice, Information sharing HM Government (2015);
- Prevent Duty Guidance: for England and Wales (March 2015) (Prevent).
- The Prevent duty: Departmental advice for schools and childminders (June 2015)
- The use of social media for on-line radicalisation (2015)
- How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE 2015)
- Cyberbullying: Advice for Heads and School staff (DfE 2014)
- Advice for parents and carers on cyberbullying (DfE 2014)
- Preventing and Tackling Bullying: Advice for school leaders and governors and the relevant aspects of Safe to Learn, embedding anti-bullying work in schools (DfE 2014)
- The DfE Don't Suffer in Silence booklet
- The Data Protection Act (2018)
- UK GDPR and Child Exploitation and Online Protection Command (CEOP).
- Teaching Online Safety in School (DfE, 2019)
- Education for a connected world (2020)
- Harmful Online challenges and online hoaxes (2021)