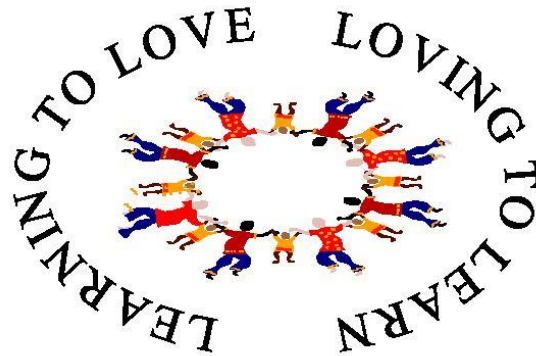


St John the Evangelist Catholic Primary School



Online Safety Policy

St. John's is a place where we meet Jesus. Everyone is enabled to fulfil their unique potential and together we celebrate being part of God's creation in all we think, say and do. In our school everyone is respected and cherished and differences are valued. Each member of our community is supported to truly reflect the person of Jesus

A Blessed Christopher Wharton Catholic Academy Trust School

DOCUMENT CONTROL

Doc Ref:	Version 2019
Document Full Title:	Online Safety Policy
Document Version Number:	February 2019
Document Stored in:	Safeguarding Support Ltd
Owned by:	Trust Board
Authorised by:	Academy Council School Governors
Date:	February 2019
Review Date:	February 2020
Circulation:	All Staff and Volunteers All School Governors All Trust Directors On Website



A Blessed Christopher Wharton Catholic Academy Trust School

Contents:

1.	Policy statement, aims and scope	p4
2.	Roles and responsibilities	p4
3.	Education	p7
4.	Internet provision	p8
5.	Filtering, monitoring and inappropriate material	p8
6.	Managing ICT systems, security and access	p9
7.	Passwords	p9
8.	Age appropriate safe use of technology	p9
9.	Personal data protection	p9
10.	Use of digital and video images (photographic and video)	p10
11.	Managing emails	p10
12.	Responding to incidents of misuse	p10
13.	Cyber-bullying	p10
14.	Social media	p11
15.	Sexting	p12
16.	Online sexual violence and sexual harassment between children	p12
17.	Online Child Sexual Abuse and Exploitation (OCSAE)	p13
18.	Indecent Images of Children (IIOC)	p14
19.	Online radicalisation and extremism	p15
20.	Mobile devices	p15
21.	Monitoring, review and impact	p16
22.	Useful information and support	p17
23.	Appendices	p18

A Blessed Christopher Wharton Catholic Academy Trust School

At St John the Evangelist Catholic Primary School, we educate our children to prepare them for this life and the next, to grow in love for God and love for their neighbour as Christ Himself. We aim for our young people to enjoy the process of unlocking their potential and experience success: to remain healthy and safe as they grow into being responsible citizens who care for others.

We are guided by these same principles in our duties to staff, parents and the wider community with due regard to legal requirements and the teaching and traditions of the Catholic Church.

Policy statement

The use of technology has become a significant component of many safeguarding issues. Therefore, this Online Safety Policy should be recognised as part of the safeguarding suite of policies and falls within the role and responsibilities of the Designated Safeguarding Lead (DSL): Sarah Kenyon and Safeguarding Governor Caroline Handley and Alison Park. This policy applies to all staff, governing body, leadership team, external agencies, visitors, volunteers, parents and those working on behalf of school, whether paid or unpaid (collectively referred to as 'staff' in this policy). It refers to all access to the internet and use of technology, including personal devices, setting devices for use off-site e.g. work laptops, tablets or mobile phones.

It takes into account the:

- DfE statutory guidance Keeping Children Safe in Education (2018)
- Early Years and Foundation Stage (2017)
- Working Together to Safeguard Children (2018)
- Prevent duty guidance (2015)
- UK Council for Internet Safety (2019)
- Bradford Safeguarding Children Board procedures

Aims and Scope

- Safeguard and protect all members of St John the Evangelist Catholic Primary School community online
- Identify approaches to educate and raise awareness of online safety
- Enable staff to work safely and responsibly to role model positive behaviour online, manage professional standards and practice when using technology
- Provide clear procedures to use when responding to online safety concerns

St John the Evangelist Catholic Primary School:

- Believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure all staff and pupils are protected from potential harm online.
- Aims to create a secure and safe environment which develops technology skills and provides staff and pupils with awareness of potential online safety scenarios that may arise
- Identifies that the internet and associated devices, computers, tablets, mobile phones and gaming consoles, are deemed important to everyday life
- Will support staff and pupils to be empowered, build resilience and develop strategies to manage and respond to online risk

Roles and responsibilities

Sarah Kenyon has lead responsibility for safeguarding and child protection, which includes online safety. Activities of the DSL may be delegated to an appropriately trained deputy, therefore activities which reference DSL also refer to deputy DSL throughout this policy. However, overall the ultimate lead for safeguarding and child protection remains with the DSL. St John the Evangelist Catholic Primary School recognise that all members of staff have important roles and responsibilities to play with regards online safety.

The Online Safety Committee:

Our school has an Online Safety Committee which is responsible for the approval and the effectiveness of the Online Safety Policy. They will meet termly to discuss, and review policies and any online safety incidents recorded within CPOMS.

A Blessed Christopher Wharton Catholic Academy Trust School

Governors:

Will do all that they reasonably can to limit pupil's exposure to the following from the school's IT system:

We identify that the issues classified within online safety are considerable, but can broadly be categorised into three areas of risk:

1. **Content** - being exposed to illegal, inappropriate or harmful material
2. **Contact** - being subjected to harmful online interaction with other users
3. **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm

The role of the Governors will include:

- Attending Online Safety Committee meetings
- Undertake a risk assessment to ensure appropriate filters and monitoring systems are in place, as required by the Prevent Duty
- Limiting pupils exposure to online risks
- Whilst considering the above they will be careful that "over blocking" does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding
- Consider a whole school approach to online safety, including a clear policy on the use of mobile technology in the school
- Ensure pupils are taught about safeguarding, including online safety and minimising the risk of peer on peer abuse e.g. sexting
- Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach
- Monitoring and reviewing online safety concerns and incidents

Headteacher and Leadership Team will ensure:

- Online safety is viewed as a safeguarding issue and that practices are in accordance with national and local requirements
- Robust policies and procedures, including the Staff Handbook and acceptable use policy are up-to-date in line with the latest guidance
- Suitable and appropriate filtering and monitoring systems are in place. Work with IT staff to monitor the safety and security of our online systems and networks
- Online safety is embedded within a broad and balanced curriculum, which enables pupils to understand age appropriate understanding of online safety
- Support the DSL by providing sufficient time and resources to fulfil their online responsibilities
- Robust and clearly understood reporting channels regarding online safety concerns, including internal, local and national support
- Appropriate risk assessments are undertaken regarding the safe use of technology
- DSL receives suitable CPD to enable them to carry out their duties and to train other staff as appropriate
- Staff are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- Audit and evaluate online safety practice, identifying strengths and areas for improvement.

Designated Safeguarding Lead (DSL) will:

- Act as named point of contact on all online safeguarding issues, liaising with other members of staff and multi-agencies, where appropriate
- Work with the deputy DSLs to ensure online safety is recognised and understood as part of St John the Evangelist Catholic Primary School safeguarding responsibilities
- Access regular and appropriate training to support staff's understanding of the unique risks associated with online safety, including how to recognise the additional risks that pupils with SEN and disabilities (SEND) may face online
- Keep up-to-date with current research, legislation and trends around online safety and disseminate this information to staff

A Blessed Christopher Wharton Catholic Academy Trust School

- Ensure all staff receive regular up-to-date and appropriate online safety training including the risks associated for pupils with SEND
- Participate in local and national events to promote positive online behaviour e.g. Safer Internet Day
- Promote online safety to parents, carers and the wider community through a variety of channels and approaches
- Maintain records of online safety concerns, recording actions, decisions and reason for decisions
- Monitor and evaluate online safety incidents to identify gaps and trends, using the findings to form response, understanding and update policies
- Report online safety concerns to the headteacher and governing body
- Support leadership team with reviewing and updating online safety policies and procedures
- Meet termly with Safeguarding Governor/Online Safety Committee

IT Technician ensures:

- The school's IT infrastructures are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- The school keeps up to date with online safety technical information and updates the DSL as relevant
- Monitoring software and antivirus software is implemented and updated
- Share any concerns with the DSL and leadership team
- Provide technical support and perspective to the DSL and leadership team, to enable them to take appropriate safeguarding action if/when required

All staff will:

- Contribute to the development of online safety policies and practices
- Read and adhere to online safety and acceptable use policies
- Keep an up to date awareness of online safety matters and the current online safety policy through staff meetings and training sessions
- Understand the procedures for reporting online safety incidents within the St John the Evangelist Catholic Primary School including recording the incident in CPOMS
- Report any suspicious misuse or problem to the DSL for investigation
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally
- Take responsibility for the security of school settings and the data they use or have access to
- Model best practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- Ensure digital communications with pupils are professional and only carried out on official school systems
- Ensure online safety issues are embedded in all aspects of the curriculum
- Ensure online safety lessons are planned and taught and that the lessons are age appropriate/reflect the needs of the age group
- Ensure pupils understand and follow the school's pupil acceptable use policy. Training should be provided on these policies at the beginning of each new academic year and for any new starters who join at a later stage
- Ensure they are aware of the online safety issues related to the use of mobile phones, cameras and mobile devices and that they monitor their use and implement current school policies with regards to these devices
- Ensure that confidential files are saved in an encrypted file and that the password for this file remains confidential
- Ensure that at the end of the academic year photographs are deleted or where applicable stored in an agreed location for school use. At the end of Year 6 all photographs are to be deleted
- Take personal responsibility for professional development in this area

Pupils will:

- Contribute to the development of online safety policies
- Take age appropriate responsibility for using the school IT systems and equipment in accordance with the pupil acceptable use policy

A Blessed Christopher Wharton Catholic Academy Trust School

- Be briefed annually on the content of the online safety policies, and asked to read and adhere to the acceptable use pupil agreement
- Respect the feelings and rights of others both on and offline
- Take responsibility for keeping themselves and others safe online
- Be encouraged through online safety/PSHE lessons to share any online safety concerns with a trusted adult.

Parents/Carers

The school will take every opportunity to help parents/carers to understand online safety issues. We will raise awareness of the key issues in the following ways:

- Information about online safety and parental resources are available
- Information is also shared via letters and newsletters

It is the responsibility of the parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them
- Support St John the Evangelist Catholic Primary School with our online safety approaches by discussing online safety issues with their children, reinforcing appropriate use of technology and online behaviour at home
- Role model safe and appropriate use of technology and social media
- Abide by the home-school agreement and acceptable use policies
- Be aware of changes in behaviour that could indicate their child may be at risk of harm
- Seek help from school or other appropriate agencies if they or their child encounter risk or concerns online
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Community users/School visitors

Community users and school visitors should speak with their school contact to discuss options available to access the school IT system and expected behaviour.

Pupil Education

The education of pupils in online safety is a crucial part of St John the Evangelist Catholic Primary School online safety provision. Pupil's need the help and support of the school to recognise and avoid online safety risks and to build their awareness of how to keep themselves safe and promote safe and responsible internet use. Online safety education will be provided in the following ways:

- Broad and balanced curriculum covering the safe and responsible use internet access
- Online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE)
- Pupils are taught in all lessons to be aware of the content that they access online and learn how to determine the accuracy of the information they find
- Provide online safety education, rules for acceptable use at the beginning of each academic year and with any new starters as they join school
- Pupils are taught how to search for information safely, including the skills of knowledge location, safe search engines and education
- Pupils are made aware of the process to follow if they see anything online which they find upsetting, or which is unsuitable for children
- Pupils know that any events of cyber-bullying are taken seriously by the [school] and they understand the importance of sharing their concerns with a trusted adult
- Inform pupils network and internet use will be monitored for safety and security and in accordance with legislation
- Use external agency support to complement and support our internal online safety approaches

St John the Evangelist Catholic Primary School recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to:

- Children in care

A Blessed Christopher Wharton Catholic Academy Trust School

- Children with SEND or mental health needs
- Children with English as an additional language (EAL)
- Children experiencing trauma or loss

We will ensure that ability appropriate online safety education, access and support is provided to vulnerable pupils. When implementing our online safety policies, we will seek input from appropriate staff, including the SENCO, Designated Teacher for Looked After and Previously Looked After Children.

Staff Education

It is essential that all staff receive regular and appropriate online safety training and to ensure they understand their responsibilities, as outlined in this policy. Training and support will be offered as follows:

- Opportunity to discuss online safety policy and procedures at induction
- Recognise the expertise staff build by undertaking training and provide opportunity for staff to contribute to and shape our policies and procedures
- Regular up-to-date online safety training, with updates at least annually covering potential risks posed to pupils (Content, Contact and Conduct) as well as expected professional practice
- Planning and online safety work will be monitored regularly and will be used to direct training
- All staff will receive a briefing and a copy of the acceptable use and online safety policy annually
- Both policies are included in the induction pack for new starters
- Make staff aware our IT systems are monitored and activity can be traced to individual users.
- Remind staff to behave professionally and in accordance with legislation and our policies when accessing our systems and devices
- Remind staff that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation
- Highlight useful age appropriate educational resources and tools for use with pupils
- Ensure staff are aware of the procedures to follow regarding online safety concerns

Governor Education

Governors are invited to take part in regular online safety training sessions with staff. Governors are aware of online safety updates through regular Online Safety Committee meetings or through subject meetings with the DSL.

Internet Provision

St John the Evangelist Catholic Primary School recognises that the internet is a constantly changing environment with new and emerging technology. The school ensures that the internet system works in accordance with Keeping Children Safe in Education guidance and makes sure appropriate filtering and monitoring systems are in place, taking reasonable precautions to ensure that users can only access appropriate material. A report is generated tracking inappropriate user activity. However, due to the global nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

Filtering, monitoring and inappropriate material

We have education broadband connectivity that blocks sites which are categorised as inappropriate or of an illegal nature.

If a pupil discovers an unsuitable site, they are required to:

- Turn off the monitor/screen and report the concern immediately to the staff member
- The staff member will report the concern (including URL of the site if possible) to the DSL or IT Technician
- The breach will be recorded and escalated as appropriate
- Parents/carers will be informed of the filtering breach involving their child
- Any material believed to be of an illegal nature will be reported immediately to the appropriate agencies.

If a concern is identified via the monitoring systems, the DSL will take appropriate action in line with our child protection procedures, recording actions, decisions and reasons for the decisions.

A Blessed Christopher Wharton Catholic Academy Trust School

All users are informed that the use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Managing ICT systems, security and access

Staff and pupils are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. All staff and pupils are required to sign our acceptable use policy before being given access to our IT systems. Access to IT systems is managed by the DSL and IT Technician.

All pupils at the school receive logins and accounts for relevant school systems. These accounts are managed through administrator privileges which are agreed by the leadership team, DSL and IT Technician. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts are deleted annually for any leavers including those children in year 6. Adult accounts and passwords are also created in the same way. Adults are given accounts for school systems, e-mail etc. Account creation and deletion are managed by the DSL and IT Technician.

St John the Evangelist Catholic Primary School takes appropriate steps to ensure the security of our information systems, including

- Virus protection is regularly updated
- Encryption of all data taken off site via portable media storage
- Not using portable media without specific permission
- Scanning portable media by an anti-virus/malware software before use
- Not downloading unapproved software or opening unfamiliar attachments
- Regularly checking files on our network
- Individual user login and passwords (expect for early years, foundation stage and some pupils with SEND)
- All users are required to log-off or lock screens if leaving them unattended

Passwords

All users (staff and pupils) have the responsibility for the security of their user name and password and must not allow other users to access the systems using their log on details (as per acceptable use policies). Any concerns about sharing passwords or log on details must be reported to the DSL.

- Use of strong passwords
- Regularly change passwords in line with school guidance
- Members of staff are made aware of the school's password rules through induction, the acceptable use policy and the online safety policy
- Pupils are made aware of the school's password rules through IT/online safety lessons and through the pupil acceptable use policy

Age Appropriate Safe Use of Technology

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional supervised access to age appropriate specific and approved online materials, which supports planned learning outcomes

Key Stage 2

- Pupils will use age appropriate search engines and online tools
- Pupils will be directed by the teacher to online materials and resources, which supports planned learning outcomes

Personal Data Protection

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full details can be found in our Data Protection and Information Sharing Policy.

A Blessed Christopher Wharton Catholic Academy Trust School

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images
- We will ensure all images and videos shared online are used in accordance with associated policies
- Staff are allowed to take digital/video images to support educational aims. These images should only be taken on school equipment. Personal equipment must not be used for these purposes.
- Parental permission to use photographs on the school website, online and in the press must be sought before posting
- Photographs will be published without names. In incidences where names are required (some newspapers) parental permission will be sought
- Teaching staff are responsible for storing photographs and images safely and securely. Staff will also ensure that images are deleted annually/once the child has left the school.

Managing emails

Access to St John the Evangelist Catholic Primary School email systems will always be in accordance with data protection legislation and our suite of policies. Staff are advised:

- Sensitive or personnel information must only be sent by encrypted email
- The forwarding of any chain messages/emails is not permitted
- School emails must not be used for personal and/or social media accounts
- Offensive communication must be reported to the DSL immediately, and will be recorded
- The use of social email should be limited to break times, before and after school hours and definitely not permitted when pupils are present.
- The use of personal email addresses by staff for any official school business is not permitted

Pupil email – whole class or group email addresses may be used for communicating outside of the school.

Responding to incidents of misuse

It is hoped that all members of staff will be responsible users of IT. However, there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Then staff should immediately notify the DSL. It is important that the device is not shut down as evidence could be erased but that it is removed to secure site.

If misuse has taken place which is not illegal it is important that any incidents are dealt with in a proportionate manner, and that members of staff are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Whilst it is impossible to record possible sanctions for every eventuality a list of types of misuse and sanctions are included in the appendix to this policy.

Cyber-bullying

Cyber-bullying, along with all other forms of bullying, will not be tolerate in St John the Evangelist Catholic Primary School. Cyber-bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, sexting, texting, use of other mobile or tablet apps, email or online software.

Pupils are taught about cyber-bullying through online safety and PSHE lessons. Pupils are encouraged to share concerns of cyber-bullying with a trusted adult. The adults in school will support the child by:

A Blessed Christopher Wharton Catholic Academy Trust School

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our anti-bullying policy. The school may report serious cyber-bullying incidents to the police.

Social Media (Staff)

The expectations regarding safe and responsible use of social media applies to all staff. All staff are expected to engage in social media in a positive, safe and responsible manner. They must keep their personal and professional lives separate on social media. Social media may include blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms – *this list is not exhaustive*.

St John the Evangelist Catholic Primary School advise staff not to publish personal opinions, detailed private thoughts, concerns, pictures or messages on any social media site, especially content that may be considered threatening, hurtful or defamatory to others. Posts must not be attributed to the school, without full permission. The use of social media should be limited to break times, before and after school hours and definitely not permitted when pupils are present.

Concerns regarding the online conduct of a member of staff on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour, staff handbook and child protection policies.

All staff are reminded that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or Trust into disrepute or if something is felt to have undermined confidence in their professional behaviour. It is the responsibility of the staff member to notify the leadership team immediately if they consider any content shared on social media sites conflict with their role and ability to work with children.

Staff are advised not to communicate with or add as friends any current or past pupils or their family members via personal social media sites, applications or profiles. Any pre-existing relationships that may compromise this must be discussed with the DSL. Staff will not use personal social media accounts to contact pupils or parents, except whereby prior approval has been given by the DSL/headteacher. Any communication from pupils and parents on social media accounts will be reported to the DSL.

The safe use of social networking and online communications will be discussed as part of the schools staff induction and throughout staff online safety training sessions. This will include:

- Setting privacy levels on personal sites
- Being aware of location sharing services
- Opting out of public listings on social network sites
- Logging out of accounts after use
- Safeguarding and strong passwords
- Not representing their personal view as that of the setting

Social Media (Pupil)

Pupils will be taught about the safe, expected behaviour, age restrictions, and appropriate use of social media as part of a broad and balanced age appropriate curriculum. Concerns regarding inappropriate pupil use of social media will be dealt with under existing safeguarding policies. This may include concerns being shared with parents/carers as appropriate.

Pupils will be advised:

- Risks associated with sharing personal data on social media sites, which could identify them and/or their location
- Only accept and invite known friends, deny access to others by making profiles private

A Blessed Christopher Wharton Catholic Academy Trust School

- Never meet any online friend without being accompanied by a trusted adult
- Use strong and safe passwords
- Only use age and ability appropriate social media sites
- How to block and report unwanted communications
- Who and how concerns should be raised in school and externally

The school's use of social media for professional purposes will be checked regularly by the Online Safety Committee to ensure compliance with this policy.

Sexting

St John the Evangelist Catholic Primary School recognises youth produced sexual imagery (known as sexting) as a safeguarding issue, all concerns will be reported to and dealt with by the DSL.

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages. Sexting can be seen as harmless but creating or sharing explicit images of a child is illegal, even if the person doing it is a child.

A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

There are many reasons why a child may want to send a naked or semi-naked picture, video or message to someone else:

- joining in because they think that 'everyone is doing it'
- boosting their self-esteem
- flirting with others and testing their sexual identity
- exploring their sexual feelings
- to get attention and connect with new people on social media
- they may find it difficult to say no if somebody asks them for an explicit image, especially if the person asking is persistent

St John the Evangelist Catholic Primary School has regard to and will follow the UK Council for Child Internet Safety guidance; Sexting in schools and colleges: responding to incidents and safeguarding young people if necessary. We will ensure all staff and pupils are made aware of the potential social, psychological and criminal consequences of sexting and how they must respond to incidents by offering specific staff and age appropriate pupil training.

Online Sexual Violence and Sexual Harassment between Children

Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.

St John the Evangelist Catholic Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

A Blessed Christopher Wharton Catholic Academy Trust School

We:

- Recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Will ensure that all staff and pupils are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- Will ensure that all members of staff are aware of sources of support regarding online sexual violence and sexual harassment between children.
- Will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL and act in accordance with our child protection and anti-bullying policies.
- If content is contained on pupils electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to Safeguarding Partners.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Online Child Sexual Abuse and Exploitation (OCSAE)

St John the Evangelist Catholic Primary School will ensure that all staff are aware of online child abuse, including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns. We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

The DSL will:

- Implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers
- Ensure support is available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- Raise pupil awareness of the importance of the 'Click CEOP' report button and where this can be accessed, e.g. websites

If made aware of an incident involving OCSAE act in accordance with our child protection and Bradford Safeguarding Children Board procedures:

- If appropriate, store any devices involved securely.
- Make a referral to the Safeguarding Partners (if required/appropriate) and immediately inform the police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of pupils(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.

A Blessed Christopher Wharton Catholic Academy Trust School

- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Safeguarding Partners
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If pupils at other setting are believed to have been targeted, the DSL will seek support from the Safeguarding Partners first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

St John the Evangelist Catholic Primary School will ensure that all staff are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- Will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Safeguarding Partners.

If made aware of IIOC, we will:

- Act in accordance with our child protection and Bradford Safeguarding Children Board procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), police or the LADO.

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- Ensure the DSL is informed
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and the Safeguarding Partners (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the headteacher is informed in line with our managing allegations against staff policy.

A Blessed Christopher Wharton Catholic Academy Trust School

- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the DSL/headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Mobile devices

St John the Evangelist Catholic Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Expectations (Staff)

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.

- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- All staff are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All staff are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in lessons, during teaching time, while on playground duty and during meetings mobile phones will be switched off or put on 'silent' or 'discreet' mode. In accordance with the acceptable use policy staff must not use personal devices for photography in school. Only school cameras or devices are to be used.

Staff are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of staff any breaches will be dealt with as part of our behaviour policy.

Mobile devices (Pupils)

School does not allow pupils to bring mobile phones into class. All mobile phones must be handed in at the start of the day and are stored in a lockable container, kept in a designated location. They will be returned at the end of the school day. Pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School mobile devices

The school has a variety of mobile devices including iPads, all the statements included in the acceptable use policy apply to these mobile devices. Staff and pupils know that they must not take pictures on school devices of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

Visitor mobile devices

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies. We will ensure

A Blessed Christopher Wharton Catholic Academy Trust School

appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL/headteacher of any breaches our policy.

Monitoring, review and impact

We acknowledge technology evolves and changes rapidly. St John the Evangelist Catholic Primary School will review this policy at least annually or following revised national or local policy requirements, child protection concerns or changes in technical infrastructure. We filter and regularly monitor internet use and evaluate online mechanisms to ensure this policy is consistently applied.

St John the Evangelist Catholic Primary School will monitor the impact of the policy using:

- Logs of reported online safety incidents
- Monitoring of network activity
- Pupil online safety survey data which is gathered through annual questionnaires during Online Safety Week
- Evaluation of children's work
- Discussions at children's groups i.e. school council
- Monitoring planning and evidence of work

Data from the above will be monitored annually and is used to develop staff training, parent coffee mornings, planning and teaching.

The DSL will ensure the headteacher is informed of any online safety concerns.

Caroline Handley and Alison Park will report on a regular basis to the governing body on online safety practices, concerns and/or incidents, including actions, decisions, reasons for those decisions and outcomes. Any identified concerns or incidents will be incorporated in our action planning

A Blessed Christopher Wharton Catholic Academy Trust School

Useful information and support

- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

A Blessed Christopher Wharton Catholic Academy Trust School

Appendices:

- 1) Sanctions for misuse (Pupils)
- 2) Sanctions for misuse (Staff)

The following policies include statements regarding Online Safety: Child Protection and Safeguarding, Staff Handbook, Acceptable Use and Behaviour.

These are available to be viewed online or within school if required.

Sanctions for misuse (Pupils)

Incident	Actions/Sanctions
Deliberately accessing or trying to access material that could be considered illegal	<ul style="list-style-type: none"> - Refer to DSL - Inform parents/carers - Refer to Police (if appropriate) - Removal of network/Internet access rights - Update CPOMS
Unauthorised use of sites, mobile devices, social networking, downloading or uploading files	<ul style="list-style-type: none"> - Refer to DSL - Inform parents/carers - Warning given - Update CPOMS
Allowing others to share usernames/passwords/using other student's accounts/staff accounts	<ul style="list-style-type: none"> - Inform DSL/IT Technician - Warning given - Update CPOMS
Corrupting or destroying the data of other users	<ul style="list-style-type: none"> - Inform DSL/IT Technician - Warning given - Update CPOMS
Sending an e-mail, text or instant message that is regarded as offensive, harassment or bullying	<ul style="list-style-type: none"> - Refer to DSL - Inform parents/carers - Removal of network/Internet access rights - Update CPOMS
Deliberately accessing offensive or pornographic material.	<ul style="list-style-type: none"> - Refer to DSL - Inform parents/carers - Refer to Police (if appropriate) - Removal of network/Internet access rights - Update CPOMS
Continued infringement of the above, following previous sanctions/warnings.	<ul style="list-style-type: none"> - Refer to DSL - Inform parents/carers - Removal of network/Internet access rights - Update CPOMS

A Blessed Christopher Wharton Catholic Academy Trust School
Sanctions for misuse (Staff)

Incident	Actions/Sanctions
Deliberately accessing or trying to access material that could be considered illegal	<ul style="list-style-type: none"> - Refer to DSL/Executive Headteacher/Headteacher/Head of School - Refer to DSL - Inform Local Authority/HR - Refer to Police (if appropriate) - Record - Suspension/disciplinary action
Unauthorised use of sites, mobile devices, social networking, downloading or uploading files	<ul style="list-style-type: none"> - Refer to DSL - Warning given - Record
Using personal email/social networking/instant or text messaging to communicate with pupils	<ul style="list-style-type: none"> - Refer to DSL/Executive Headteacher/Headteacher/Head of School - Inform Local Authority/HR - Record - Suspension/disciplinary action
Allowing others to access school network by sharing username and passwords or using another person's account.	<ul style="list-style-type: none"> - Refer to DSL - Warning given - Record
Sending an e-mail, text or instant message that is regarded as offensive, harassment or bullying	<ul style="list-style-type: none"> - Refer to DSL/Executive Headteacher/Headteacher/Head of School - Inform Local Authority/HR - Record - Warning/Suspension
Careless use of personal data e.g. holding or transferring data in an insecure manner	<ul style="list-style-type: none"> - Refer to DSL/Executive Headteacher/Headteacher/Head of School - Warning given - Record
Deliberately accessing offensive or pornographic material.	<ul style="list-style-type: none"> - Refer to DSL/Executive Headteacher/Headteacher/Head of School - Refer to Police (if appropriate) - Removal of network/Internet access rights - Record
Continued infringement of the above, following previous sanctions/warnings.	<ul style="list-style-type: none"> - Refer to DSL/Executive Headteacher/Headteacher/Head of School - Inform Local Authority/HR - Removal of network/Internet access rights - Record - Suspension/ disciplinary action