St Joseph's High School



E-Safety Policy

Review Date: March 2026

Content Page

1. **Introduction**

   The E-Safety Policy

   Aims

   Computer Network Security

   Review

   Internet Filtering

2. **Online Harms and Reporting**

   Online Child Sexual Abuse

   Child sexual abuse material

   Sharing nudes

   Personal Electronic devices

   Talking to a child about keeping safe online

   Online Grooming

   How to respond to suspected grooming

   Online blackmail

   Harmful content

   Pornography

   Extreme pornography

   Effects on children

   Voyeurism

   Self-harm and suicide

   Online bullying

   Signs of bullying

   How to help a child experiencing online bullying

   Responding to online bullying incidents

   Preventing Bullying

   Other offences committed online

   Domestic Abuse

   Stalking

Threatening or abusive behaviours

Harassment

Putting people in fear of violence

Malicious communications

Hate crime

Online gaming

Online radicalisation extremism

Setting up a new planform safety

3. **Social networking**

4. **Handling E-safety complaints**

The E- Safety Policy
This E-safety policy relates to other major school policies, which can be viewed on the school's website, and include:

- Child Protection Policy
- Anti-bullying Policy
- Acceptable Use of the Internet Policy
- Bring Your Own Device to School Policy
- Mobile Phone/I
- Code of Conduct
- Staff Code of Conduct
- Complaints Policy

It has been written by the school's Pastoral Vice Principal in conjunction with the Head of ICT, ICT Technician, Designated Teacher for Child Protection and Teacher in Charge of E-Learning

The policy has been agreed by the Senior Leadership Team and approved by the Board of Governors.

Aims of the policy

The aim of this E-Safety policy is to ensure that pupils will benefit from learning opportunities offered by the school's electronic resources in a safe and effective manner. E-safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
E-safety depends on effective practice at a number of levels:

- sound implementation of an agreed, comprehensive E-safety policy, in both administration and curriculum
- education for responsible ICT use by staff, pupils and families
- Safe and secure broadband, including the effective management of filtering

Computer Network Security

The C2K network used in St Joseph's is managed and maintained by the C2K support team in the EA along with Capita who is responsible for the hardware and the security of the system.

The following protocols are enforced by the school to comply with security regulations:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly. Portable media will be scanned with anti-virus / malware software. Any device which has a virus will be denied access.
- Unapproved software will not be allowed in work areas or attached to email. Files held on the school's network will be regularly checked.
- C2k/IT Technician will review the system capacity regularity. The use of user Logins and passwords to access the school network will be enforced.

Review

The E - Safety policy and its implementation will be reviewed annually by the Designated Safeguarding Teacher(s) in conjunction with the ICT HOD. The policy should be reviewed every year, or sooner if deemed necessary due to significant changes in legislation or government guidance on online safety, or because of any other significant event or safeguarding incident

Internet Filtering

The sole internet provider for pupil use in St Joseph's is the C2k connection. Pupils who access the Internet using eg 4G/5G or other broadband connections while in school are in breach of the school rules. The school's positive behaviour policy will be followed.

The C2k Internet filtering system has a filtering system which provides an effective defence against inappropriate websites. C2K define three types of access:

GREEN accessible to all users in schools

AMBER accessible to school's selected groups of users (can be changed by the C2K Manager)

RED not accessible to any user

An Internet filtering service, no matter how thorough, can never be completely comprehensive. To deal with this issue the school enforces the following rules/procedures:

- Internet sessions will be supervised by a member of staff where possible.
- Pupils' Internet usage is regularly monitored

- Pupils will be aware that any usage, including distributing or receiving information, may be monitored for unusual activity, security and/or network management reasons.

  Pupils will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Pupils and staff will report accidental accessing of inappropriate materials in accordance with school procedures.

Online harms and reporting

Online harms are user-generated content or behaviour that is illegal or could cause significant physical or psychological harm to a person. Online harms can be illegal, or they can be harmful to a child or young people, but still be legal. It is essential that children, in particular, are safeguarded from potentially harmful and inappropriate online material.

Examples of online harms include:

- Online child sexual exploitation or grooming
- Viewing harmful content
- Sharing nudes
- Online bullying
- Online gambling

The breadth of issues classified within online safety is considerable and ever-evolving, but can be categorised 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:** 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.

Online Child Sexual Abuse

Sexual abuse can happen online as well as offline and includes:

- Showing pornography
- Exposing a child to sexual acts
- Forcing a child to make, view, or share child abuse images or videos
- Making, viewing, or distributing child abuse images or videos
- Forcing a child to take part in sexual activities or conversations online
- Blackmailing a child to share their images unless they pay out money

Online child sexual exploitation occurs when a child is sexually exploited online. They may be persuaded or forced to create sexually explicit photos or videos or have sexual conversations.

The internet has not created child sexual abuse, but it makes it easier for adult offenders to contact and groom children and young people. When contacting a child online, an adult offender's objective might be to meet them face to face to abuse them. Many offenders, however, abuse children without meeting them by forcing or tricking them into producing and sharing sexual images or videos or engaging in sexual activity on camera or livestream.

If information is received by any agency, organisation, or practitioner which suggests a young person is being sexually exploited, or at risk of sexual exploitation, a report should be made to the relevant HSCT or PSNI and a child protection investigation should be conducted in compliance with the requirements of the Joint Protocol. The PSNI must be involved as early as possible in the investigative process to ensure any evidence that may assist prosecution is not lost, and to enable a disruption plan to reduce the victim's contact with the perpetrator(s) and reduce the perpetrator(s) control over the victim(s) to be put in place without delay. Once concerns have been reported, the HSCT and the PSNI must ensure that urgent action is taken to protect the child and safeguard the child from any continuing risk of harm.

Staff should always remain vigilant and observant to this type of abuse. Offenders of child sexual abuse come from all walks of life. Perpetrators, although predominantly male, can also be female, young, or old, and from any social or cultural background. They can abuse children of any gender, age, and social or cultural background. They can also be people that the child knows.

Child sexual abuse material

Child sexual abuse material is a result of children being groomed, coerced, and exploited by their abusers, and is a form of child sexual abuse. It is important to use the correct term 'child sexual abuse material' and not 'child pornography' which implies it is a sub-category of legally acceptable pornography, rather than a form of child abuse and a crime.

It is a serious criminal offence against children to take, make, distribute, or possess an indecent photograph or pseudo-photograph of a child under the age of 18.

Child sexual abuse material can remain online indefinitely, therefore children continue to be re-victimised each time it is viewed, shared, or downloaded. Children who have been abused in this way may grow up with feelings of shame, guilt, humiliation, and fear that abuse materials may resurface in future, giving them no sense of closure for the crimes committed against them.

Sharing nudes

Sharing nudes or semi-nudes is a term used to describe when persons under 18 send or post nude or semi-nude images, videos, or livestreams online. Professionals might use the term sexting, youth-produced sexual imagery, or self-generated indecent imagery. Young people might use terms such as nudes, pics, or dick pics.

It is illegal to take, possess, or share nude images of anyone under 18 and it is important that young people are aware of this. The legislation was created to protect and safeguard children from abuse, it was not created to criminalise them. Staff responding to incidents of sharing nudes and semi-nudes is complex because of its legal status. Staff should be alert to their legal obligations including reporting of offences - Section 5 of the Criminal Law Act (NI) 1967 makes it an offence to fail to report a relevant offence. This includes children sharing nudes and semi-nudes.

Even if a young person has technically committed an offence, the matter will be dealt with sensitively by the police, who will take into consideration all the circumstances. However, young people who pressure other under 18s to share nudes and semi-nudes, or intentionally share or threaten to share intimate images or films without consent are committing a serious offence.

Finding a sensitive and supportive way to deal with the situation is the goal. A child or young person may be feeling embarrassed or distressed and it can be difficult for adults to know what to say and do. The quicker you can respond the more control you have.

Police Service of Northern Ireland advice is that if you receive what you believe to be an indecent image, do not delete it and contact the Police as soon as you can. You must not send this image to another person or show it to anyone else as you may be committing an offence.

Personal Electronic devices

Mobile phones and other Internet enabled personal devices can be used to communicate in a variety of ways. Mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged
- Their use can render pupils or staff subject to cyber bullying
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering. (VPN) The use of VPN'S Virtual Personal Network is strictly prohibited Kids are using this
- They can undermine classroom discipline as they can be used on "silent" mode
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

The school employs a strict policy on the use of mobile phones on school premises between 8.30 am. and 2.35 pm. Guidelines and sanctions are outlined in the school's Mobile Phone Policy. The following points outline the e safety guidelines for mobile phones/personal devices:

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy and may also be a criminal offence.
- Mobile phones and personal devices will not normally be used during lessons or formal school time unless under the direction of a member of staff for educational purposes.
- The Bluetooth function of all devices should be switched off at all times and not be used to send images or flies to other devices.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Talking to a child about keeping safe online

Having early, often, and open conversations with a child or young person about their online activity can help them understand who to trust online and empower them to

avoid or safely deal with inappropriate contact. E-Safety modules are delivering in ICT from Year 8 and through The Internet Safety Week, workshops etc.

Further advice on sharing nudes can be found on the Online Safety Hub.

Online Grooming

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation, or trafficking. Children and vulnerable adults can be groomed online or face-to-face, by a stranger or by someone they know, for example, a family member, friend, or professional. Groomers may be male or female of any age.

It can be difficult to tell if a child is being groomed as the signs are not always obvious and may be hidden. Older children might behave in a way that seems to be "normal" teenage behaviour, masking underlying problems. A child is unlikely to know they've been groomed. They might be worried or confused and less likely to speak to an adult they trust.

Some of the signs you might see include:

- Being very secretive about how they're spending their time, including when online
- Having an older boyfriend or girlfriend
- Having money or new things like clothes and mobile phones that they can't or won't explain
- Underage drinking or drug taking
- Spending more or less time online or on their devices
- Being upset, withdrawn, or distressed
- Sexualised behaviour, language, or an understanding of sex that's not appropriate for their age
- Spending more time away from home or going missing for periods of time

---

How to respond to suspected grooming

Grooming is a criminal offence and occurs where an adult communicates with a person with a view to grooming a child (The Sexual Offences (Northern Ireland) Order 2008).

If there are suspicions that a child has become at risk from online grooming it is important to listen, reassure and report. Try not to panic and remember the following:

- Report any concerns to the police on 101, report it online or phone 999 in an emergency.
- Keep evidence. Keep a record of what has been happening. Take screenshots and save messages. This will help you to prove what has been happening when reporting.
- Ask the child to end all communication with the person who is grooming them, and block the person on all platforms and devices.

Further advice on online grooming can be found on the Online Safety Hub.

Online blackmail (sextortion)

Online blackmail is when someone threatens to share private information, images, or videos of a person online unless something is done for them. Young people sometimes send nude pictures or videos to flirt or have fun with other people online. These people might be known to young people in person or only online. Young people may believe that images and videos will not be shared any further. Unfortunately, there are some offenders online who will try to trick or pressure young people into sending nude images or videos of themselves. This can happen through their favourite social media app, website, or platform.

Once an offender has a nude image or a video, they may threaten to share it publicly, unless the young person meets a financial demand (Financially Motivated Sexual Extortion – often referred to as 'Sextortion').

'Sextortion' may present as:

- Financial blackmail using sexual/indecent images that have been sent to an offender a child or young person has had contact with online.
- Financial blackmail using images that have been stolen from a child or young person, taken through hacking or have been faked using image altering technology.
- Blackmail using sexual/indecent images that a child or young person has sent to an offender, but with a demand for something other than money. This might be a demand for them to do something they don't want to, like give them use of your bank account. Sometimes the offender may ask for more nude images.

If you think a young person is experiencing online blackmail report it to the police by calling 101 or 999 in an emergency.

Further advice on online grooming can be found on the Online Safety Hub.

Harmful content

As children start to explore the internet, they may come across content that isn't suitable for their age, or that may upset or worry them.

Harmful content can include:

- Sexual content, including pornography
- Violent content
- Fake news
- Hate speech

Content may be legal but could be harmful to a child. Harmful content can depend on a child's age, development, maturity, and support.

Pornography

Having, sharing, or selling adult pornography is, as a general rule, not illegal. However, some pornography is illegal and possessing, making, or distributing it are serious offences.

Legal adult pornography is readily available online. It can be found via search engines, but often it appears in pop-ups. It is not illegal for someone under the age of 18 to watch pornography, it is illegal for someone to show, or give access to pornography to anyone under 16.

Extreme pornography

It is illegal to possess 'extreme pornographic images'. This is material that's 'grossly offensive, disgusting or otherwise obscene', and that 'explicitly and realistically' shows:

- Life-threatening injury
- Significant injury to a person’s anus, breasts, or genitals
- Bestiality (a sexual act with an animal)
- Necrophilia (a sexual act with a human corpse)
- Rape or assault by penetration

Effects on children

- Normalisation of extreme or risky sexual acts
- More likely to engage in harmful sexual activity
- Developing discriminatory attitudes
- Inability to engage in real-life relationships
- An unhealthy preoccupation with pornography which can interfere with other aspects of life

Some young people speak of being "obsessed" or "addicted" to certain online material, most notably pornography. For some, visiting adult sites had become part of their daily routine. St Joseph's staff should be aware of children's use of the internet whilst in the building and interacting online and any concerns should be forwarded to the DESIGNATED TEACHERS/Designated Teacher.

Voyeurism

Direct observation of another adult or child without their knowledge, when a reasonable level of privacy is expected. This includes, but is not limited to, cameras being set up in communal areas such as toilets, and private areas such as bedrooms, in order to record someone engaging in a private act (e.g., taking their clothes off or engaging in sexual activity). It also includes viewing live footage of another individual engaging in voyeuristic activities.

Upskirting, downblousing, and cyberflashing are specific criminal offences in Northern Ireland.

- **Upskirting** is when someone uses a mobile phone or mirror to observe or take a photograph/recording under a person's clothing without their consent with the intention of obtaining sexual gratification, or to cause humiliation, distress, or alarm.
- **Downblousing** is when someone uses a mobile phone or mirror to observe or take a photograph/recording down somebody's top without their consent with the intention of obtaining sexual gratification, or to cause humiliation, distress, or alarm.
- **Cyberflashing** is when someone sends an unsolicited sexual image to a person without their consent via digital methods such as social media or dating apps.

Staff should raise any concerns with the DESIGNATED TEACHERS/Designated Teacher immediately if they suspect an offence is being committed.

Self-harm and suicide

Many online forums, social media, messaging apps, and websites can glorify, reinforce, or encourage self-harming or suicidal behaviour. Content includes information, pictures, or videos on how to self-harm and describe ways in which children and young people can take their own lives.

The reasons children and teenagers can self-harm are often complicated and will be different for every child or young person. Sometimes a child or teenager may not know the reasons they self-harm. For many young people, self-harm can feel like a way to cope with difficult feelings or to release tension. The physical pain of hurting themselves can feel like a distraction from the emotional pain they're struggling with.

Some difficult experiences or emotions can make self-harm more likely in children:

- Experiencing depression, anxiety, or eating problems
- Having low self-esteem or feeling like they are not good enough
- Being bullied or feeling alone
- Experiencing emotional, physical, or sexual abuse, or neglect
- Grieving or having problems with family relationships
- Feeling angry, numb, or like they do not have control over their lives

Any concerns about a child or young person should be communicated to the Designated Teachers.

Online bullying

Online bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone" Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying. There are clear procedures in place to support anyone in the school community affected by cyber bullying:

- All incidents of cyber bullying reported to the school will be recorded.
- All incidents or allegations of cyber bullying will be fully investigated.
- Pupils, staff and parents/carers will be advised to keep a written record of the bullying as evidence.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos.

Most cases of online bullying happen outside school, meaning schools are not always able to take direct action. Schools can put in place measures which may help to prevent online bullying occurring outside of school hours. For example, pupils may learn/be given advice about online behaviour and its risks through the school curriculum and by taking part in activities for Anti-Bullying Week and Safer Internet Day. Schools should set out their responsibilities within a separate Anti-Bullying Policy.

Online bullying, often referred to as cyberbullying, can occur on any type of device connected to the internet, including social networks, gaming, and websites.

Some examples:

- Abusive or threatening messages or emails
- Abusive comments on social media
- Sharing humiliating videos or pictures of someone
- Spreading rumours online
- Trolling – the sending of menacing or upsetting messages on social networks, chat rooms, or online games
- Excluding children from online games, activities, or friendship groups

---

Signs of bullying

No single sign will indicate for certain that your child's being bullied, but watch out for:

- Belongings getting 'lost' or damaged
- Physical injuries, such as unexplained bruises
- Being afraid to go to school, being mysteriously 'ill' each morning, or skipping school
- Not doing as well at school
- Asking for, or stealing, money (to give to whoever is bullying them)
- Being nervous, losing confidence, or becoming distressed and withdrawn
- Problems with eating or sleeping
- Bullying others

How to help a child experiencing online bullying

- Reassure them you are there to help

- Speak to a member of staff at their school or club etc.
- Help them to block and report
- Show them how to save evidence by taking screenshots
- Remind them never to retaliate
- Let them know they can always talk to you or Childline

Responding to online bullying incidents

If a child or young person is experiencing bullying in an online setting, report it to the social media or gaming platform. You can also contact 101 for advice from the police as some behaviour may break the law.

- Listen to all the children involved to establish what has happened
- Record details of the incident and any actions you have taken
- Inform the Designated teachers
- Inform parents and carers (unless doing so would put a child at further risk of harm)
- Provide support to the child/children being bullied, children who witnessed the bullying, and the child/children who has been accused of bullying
- Ask the child/children who have been bullied what they would like to happen next
- Consider appropriate sanctions for children that have conducted bullying
- Continue to monitor the situation even if the situation has been resolved

If you need guidance and support on issues affecting children you can contact the NSPCC helpline on 0808 800 500 or email help@nspcc.org.uk.

Other contacts:

- Text-A-Nurse: A text messaging service for parents and carers to access professional nursing advice on young people's health and wellbeing issues.
- Parentline: A free and confidential helpline and online chat service for parents and carers in Northern Ireland.
- Parenting Focus: Provide a free support line and webchat for parents and carers in Northern Ireland.
- Childline: If you require help and support in confidence, you can call Childline on 0800 1111. You can find additional resources on bullying and cyberbullying on their website.
- Lifeline: Northern Ireland's crisis response helpline. If you, or someone you know, is in distress or despair, call Lifeline on 0808 808 8000. This is a confidential service, where trained counsellors will listen and help immediately

on the phone and follow-up with other support if necessary. The helpline is available 24 hours a day, seven days a week.
- Youth Wellness Hub
- Anti-Bullying Alliance

Preventing Bullying

Organisations should build in contextual safeguarding considerations into their operating systems and risk assessment, including:

- Consider whether there are any areas where bullying may be more likely to happen, e.g., toilets or unsupervised areas.
- Staff awareness of dynamics of children's relationships.
- Talking to children and young people where suspected issues arise.

Organisations aim to create an inclusive and supportive environment where children, young people, and adults treat each other with respect. As part of this, staff and volunteers should challenge inappropriate behaviour or language and not dismiss it as 'banter'.

Other offences committed online

It is important to note that children and young people under 18 years can be victims of criminal offences outlined below. If these offences are suspected to be committed against a child or young person this should be reported to the police on 101 (999 in an emergency).

Domestic Abuse

The offence of domestic abuse criminalises patterns of physical and/or psychological abuse by a partner, ex-partner, or close family member. It covers behaviour that is physically violent, threatening or intimidating, as well as behaviour that is controlling or coercive or amounts to psychological, emotional, financial, online or technological abuse. Online and technological abuse is where abusers exploit the use of technology, social media, or other online means to control or coerce victims.

Stalking

The offence of stalking occurs when anyone engages in a course of conduct which causes, intends to cause, or ought to know that it will cause another person to suffer fear, alarm or substantial distress, commits the offence of stalking.

Stalking can also be carried out online using any type of electronic communication for example the sending of unwanted or malicious emails or text messages, posting messages on social media, creating fake social media profiles.

If the behaviours are fixated, obsessive, unwanted and repeated causing, or intending to cause, fear, distress, or anxiety, then it is stalking.

It is important to note that children and young people under 18 years can be victims of stalking.

Threatening or abusive behaviour

A person commits the offence by behaving in a threatening or abusive manner, and intends by that behaviour to cause, or the behaviour is likely to cause, another person to suffer fear or alarm.

There is a range of behaviours that can be considered as threatening or abusive, which includes online activity such as publishing or threatening to publish personal information or images relating to the victim, using multiple social media accounts, email addresses or phone numbers to contact the victim, creating social media posts or websites containing malicious or personal content relating to the victim, or referencing things which would have meaning only to the victim.

Harassment

The offence of harassment (Protection from Harassment (Northern Ireland) Order 1997) occurs when a person pursues a course of conduct on at least two occasions which amounts to harassment of another and which the perpetrator knows, or ought to know, will cause the victim harassment, including alarming the person or causing them distress. Behaviour can be online as part of a campaign of harassment including frequent, unwanted contact, via telephone calls, text messages, emails or other contact such as via the internet or social networking sites.

Putting people in fear of violence

The offence of putting people in fear of violence (Protection from Harassment (Northern Ireland) Order 1997) is committed when a person's course of conduct on at

least two occasions causes another to fear, on at least two occasions, that violence will be used against them, which includes online activity.

Malicious communications

This offence includes communications sent via social media, text messages or email when a person sends to another person a letter or other article which conveys a message, which is indecent or grossly offensive and the intention is to cause distress or anxiety to the recipient. The content of the communication can be a threat; information which is false and known or believed to be false by the sender; or any other article which is, in whole or part, of an indecent or grossly offensive nature.

The Communications Act 2003 also makes it an offence to use public electronic communications networks to send a message or any other matter that is grossly offensive or menacing.

Hate crime

Hate crime is a criminal offence committed against a person usually because of their (perceived) race, religion, sexuality, or disability. Hate crime can take many forms from bullying and name-calling, damage to property, violent attacks and even hate mail.

Online gaming

Online games can be a great way for children and young people to keep busy and stay in touch with friends and family, but it is important that they play safely.

Gaming can be a positive thing providing a way for children to relax, socialise, learn new skills, be part of a team. However, it also carries risks:

- Grooming by online predators
- Online bullying
- Violent content extreme violence, warfare, and criminal activity
- Show explicit sexual acts, which may glamourise rape and sexual assault
- Use racist, homophobic, or sexist language, or swearing
- Depict certain groups such as women in a derogatory way
- Gambling

More information on the risks of online gaming and a short video can be found on the NSPCC website.

Online radicalisation and extremism

Children can be exposed to different views and receive information from various sources. Some of these views may be considered radical or extreme. Radicalisation is the process through which a person comes to support or be involved in extremist ideologies. It can result in a person becoming drawn into terrorism and is a form of harm.

It is important that your organisation recognises its responsibility to challenge and report radical or extreme content as part of a shared effort to challenge and tackle extremism.

You can seek advice by:

- Contacting the Designated teachers
- Calling the NSPCC Helpline 0808 800 5000 or email help@nspcc.org

If you think a child or the people around them are involved in radicalisation report your concerns to the police on 101, report it online or phone 999 in an emergency.

Setting up a new online platform safely

Using online platforms for online events has many benefits, such as livestreaming or running virtual events. St Joseph's High School will always carry out a full risk assessment of any new platform or existing platform before the event to ensure that it is safe and has appropriate steps in place to help mitigate any risk to children or young people.

The following points should be considered:

- **Be clear about its purpose:** You should be clear about why the platform is being used and whether it is necessary.
- **Make sure it is age appropriate:** Always make sure that the platform used is suitable for the age of children, their stage of development and ability. Most social media sites have age-ratings of 13+, but some livestream apps are often 18+. It

might be that consideration needs to be given to having a parent or carer on the call to supervise the child, or appropriate parental consent.

- **Test out communication features:** Platforms often have multiple features to allow people to share, talk and see each other. Consider if the platform allows children or young people to be contacted, and whether these features are moderated, or accessible outside the hours where moderation takes place.
- **Explore safety and privacy settings:** Only use a platform that has clear guidance and advice about how the platform can be kept safe for children and young people.
- **Consider staff roles and responsibilities:** Platforms should have a member of staff responsible for moderating the platform when it is being used by children or young people. This is to prevent inappropriate content from being shared on the platform and help keep them safe.

Checklist:

- ✓ Explore safety tools and settings available
- ✓ Test out the communication features
- ✓ Ensure all appropriate safety and privacy tools have been enabled before use
- ✓ Make sure staff, volunteers use your organisation email address
- ✓ Ensure staff, volunteers, parents, carers, and children know how to report online safeguarding incidents
- ✓ Ensure all staff have read and understand the code of conduct
- ✓ Consider how the safeguarding lead will monitor the platform

Social Networking

This should be read in conjunction with the school's Staff Code of Conduct.

Social networking sites can connect people with similar or different interests but can also pose a number of dangers. All staff and pupils will be made aware of the potential risks of using social networking sites outside of school. They will be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their status.

The following guidance is given to all members of the school community regarding the use of social networking sites which should only be accessed outside of school hours:

- The use of social network spaces outside school is illegal and deemed to be inappropriate for pupils under the age of 13
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications

- Pupils should never give out personal details which may identify them, their friends and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils are advised to use nicknames and avatars (icons or computer characters) when using social networking sites
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory or bring the name of St Joseph's High School into disrepute. Criminal proceedings may be brought to bear in cases where this rule has been contravened. Concerns regarding pupils' use of social networking, social media and personal publishing sites (out of school) will be raised with their parents/carers if it impacts on the school community.
- Staff educational Blogs or Wikis should be password protected and monitored very closely. Any breach in security or inappropriate material being published should be immediately reported to the Senior Management Team
- Staff's personal use of social networking, social media and personal publishing sites will be discussed as part of staff training days and will be outlined in the Staff Code of Conduct.

Handling E-safety complaints

- All members of the school community will be informed about the procedure for reporting e-safety concerns
- All incidents and actions concerning e-safety will be recorded.
- The school will manage e-safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- Complaints of a child protection nature must be investigated in accordance with the school's Child Protection policy and will be led by the Designated Teacher for Child Protection.
- The school will inform parents/carers of any incidents of concerns as and when required.
- Any complaint about staff misuse must be referred to the principal.
- Parents will be informed of the school's Complaints Policy, available on the school website.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Sanctions

Misuse of the Internet/electronic resources or damage to the school's good name may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school will report any illegal activities to the appropriate authorities.

Please review the E Safety Agreement, sign and return to your child's Form Teacher.

Parental E -Safety Agreement

Name of pupil: _____

Class: _____

As the parent/legal guardian of the above named pupil, I confirm that I have read and agree with the school's E-Safety Policy. I understand that any breach of the school's E Safety Policy could result in a withdrawal of the facility/other disciplinary action.

I also give permission for my child's photograph/work to be published on the school website.

Parental signature: _____

Date: _____

(Only to be completed if you do not wish your child to have Internet access)

I do not grant permission for my child to be given access to the school's Internet systems and understand that this may restrict their learning opportunities.

Parental signature: _____

Pupil E- Safety Agreement

Name of pupil: _____

Class: _____

As a pupil of St Joseph's High School, I confirm that I have read and agree with the school's E-Safety Policy and understand it is to keep me, my family and friends safe. I understand that any breach of the school's E Safety policy could result in a withdrawal of the facility/other disciplinary action.

I agree to follow the school's E-Safety Policy on the use of the Internet and to use the Internet in a safe and responsible way.

Pupil signature: _____

Date: _____