St Edward's Catholic First School

E SAFETY POLICY

E Safety Policy
FGB Approval
Ratified: February 2026
Review: February 2027

ST EDWARD'S CATHOLIC FIRST SCHOOL

St Edward's Catholic First School strives to provide a broad, balanced, and relevant Catholic education in which we recognise, through mutual respect, and our mission statement that *We See Jesus in Everything We Do.*

STATEMENT

The Governors of St Edward's Catholic First School are fully aware and responsive to the needs of our whole school community with regards to E-Safety.

We understand that the risks posed in today's ever-changing society can present dangers, not just to the children within our care, but to the staff and adults that work within our school environment.

It is the responsibility of the Governors and Senior Leadership Team (SLT) of St Edward's Catholic First School to ensure that we have in place the means to protect all children and staff, together with the wider workforce and ensure that they know how to avoid unnecessary risks and where to go to seek help and advice should they feel vulnerable or threatened.

We will continue to monitor the ever-changing digital world to ensure that we are as knowledgeable and pro-active as we as can be to minimise potentially harmful situations for our school and those within it and we will continue to take advice from outside agencies, to ensure we are taking every possible opportunity to keep our pupils and adults safe.

The responsibility for E-Safety will now form part of Safeguarding and both policies should be read in conjunction with each other.

However, we will continue to promote the valuable resource provided by technology, but in a safe and protective environment and ensuring that we have the appropriate mechanisms in place to ensure that this is done safely and responsibly.

Whilst this policy is specific to St Edward's Catholic First School, the appendices included are those recommended by the Local Authority in their E-safety Exemplar Policy and Guidance 2012 where appropriate.

This policy should also be read in conjunction with the Berkshire Local Safeguarding Children Board Child Protection Procedures (http://proceduresonline.com/berks/).

POLICY CONTENT

APPENDICES

1. BACKGROUND

E-safety is defined as being safe from risks to personal safety and well-being when using all fixed and digital devices that allow access to the internet as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones, smart watches and gaming consoles.

E-Safety is a shared responsibility within our school community and each person has an active role to play in ensuring that risk is minimised. This policy is available and easily accessible on the school website to ensure that staff, students working in school, pupils, families and the wider community can use the information provided to maintain a safe environment not just for themselves but for the children we and they are responsible for.

2. DUTY OF CARE BY ORGANISATIONS

As part of Every Child Matters agenda set out by the Government (Education Act 2002 and the Children's Act 2004) and the 'No Secrets' agenda produced by the Government in 2000 it is our responsibility to ensure that all members of our community from the youngest to the eldest are protected from harm.

With an ever-changing environment it is not possible to provide a 100% guarantee of safety, however we take our responsibility seriously to minimise risk and do all we reasonably can to protect our community and most especially the children within it. We will ensure that we use 'managed' systems i.e. systems where children can learn to assess and manage risks for themselves.

We have a duty of care to ensure that we teach every pupil how to keep themselves safe and that if they do not feel safe what they can do.

We will provide time in which to teach every age group about their own personal safety see Appendix A, B, C, D, F and H – this may be during assemblies (including inviting 'experts' to come speak to the children), lesson time and focus 'days' in addition to IT lessons.

A dedicated E-Safety assembly is shared with all children and we will continue to provide information for children and parents on our school website as well as provide links to specific websites which can offer further advice. This information is also regularly included in the school newsletter as and when information is updated.

We will endeavour to engender a sense of responsibility within our pupils which will ensure that they can remain 'safe' not just in school but in their own time and other locations.

We also have a duty of care to the adults within our setting that they are aware of safe practices so that they are safeguarded from misunderstanding or being involved in

allegations of inappropriate behaviour. This will be done via staff induction and staff meetings.

3. THE RISKS

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life-skill, is vital to access life-long learning and employment.

While acknowledging the benefits, we recognise that risk to safety and well-being of users is everchanging as technologies develop. These can be summarised as the 3Cs:

Content

- Commercial (adverts, spam, sponsorship, personal information)
- Aggressive (violent/hateful content)
- Sexual (pornographic or unwelcome sexual content)
- Values (bias, racism, misleading info or advice)

Certification

- Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism that would be considered *inappropriate and restricted* elsewhere.

Cyberbullying

- Bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or
  anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as 'grooming' and may take place over a period of months using chat rooms, social networking sites and mobile phones.

4. ACCEPTABLE USE POLICIES (AUPS)

St Edward's Catholic First School has an acceptable use policy designed to ensure that all staff and adults within the school understand the requirement for acceptable use of all equipment, both school and personal and the requirements of the SLT and Governors to ensure they are only used when appropriate and responsibly.

See Appendix F and J. In order to ensure the safety of all pupils' parents are also asked to complete a 'Use of Camera and Video Code'.

5. E-SAFETY LEAD

The E-safety Lead will ensure that e-safety is given a high priority and that it is continually monitored.

There is also a designated Governor with responsibility for e-safety who will be the Safeguarding Designated Governor.

The responsibilities of the e-safety lead will be: -

- Maintaining the AUPs
- Ensuring that the organisation's policies and procedures include aspects of e-safety.
- Working with the filter system provider to ensure that the filtering is set at the correct level for staff, children, young people and vulnerable adults
- Report issues to the head of the organisation
- Ensure that staff participate in e-safety training
- Ensure that e-safety is included in staff induction
- Monitor and evaluate incidents that occur to inform future safeguarding developments
- Lead a whole school assembly

6. MANAGING INCIDENTS

The e-safety lead/safeguarding lead will ensure that an adult follows these procedures in the event of any misuse of the internet.

See Appendix H for the legal frameworks associated with this policy and Appendix K referring to Searching and Deletion.

<u>Has there been inappropriate contact?</u>

1. Report to the organisation manager/e-safety lead/Designated Safeguarding Lead
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3. Contact the parent(s)/carer(s)
4. Contact the police on 101
5. Log the incident
6. Identify support for the child, young person or vulnerable adult

<u>Has someone been bullied?</u>

1. Report to the organisation manager/e-safety lead/Designated Safeguarding Lead
2. Advise the child, young person or vulnerable adult not to respond to the message

3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or repetitious nature
   of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Has someone made malicious/threatening comments? (child/young person/vulnerable adult or organisation staff/volunteer)

1. Report to the organisation manager/e-safety lead/ Designated Safeguarding Lead
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Has an inappropriate/illegal website been viewed?

1. Report to the organisation manager/e-safety lead/ Designated Safeguarding Lead
2. If illegal (See Appendix F), do not log off the computer but disconnect from the
   electricity supply and contact the police on 101
3. Record the website address as well as the date and time of access
4. If inappropriate (See Appendix F), refer the child/young person/vulnerable adult to
   the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s)
7. Contact the filtering software provider to notify them of the website
8. Log the incident
9. Identify support for the child, young person or vulnerable adult

Has an allegation been made against a member organisation staff/volunteer?

Child/Young People Organisation

In the case of the above, the Berkshire LSCB Child Protection Procedures should be referred to (http://proceduresonline.com/berks/).

All allegations should be reported to the organisation manager, police (101) and the Local Authority Designated Officer (LADO) (01344 352020), as appropriate.

Vulnerable Adult Organisation

In the case of the above, the Berkshire Safeguarding Adults Policy and Procedures should be referred to (www.sabberkshirewest.co.uk/practitioners/berkshire-safeguarding-adults-policy-and-procedures).

All allegations should be reported to the organisation manager, police (101) and the Community Response and Re-enablement Team (01344 351500), as appropriate.

See Appendix K for Further Guidance.

Note: Please refer to Appendix F for a summary of what constitutes inappropriate and illegal acts involving the internet and electronic communication technologies. Further advice and guidance are shown below.

Children and Young People

To discuss an e-safety concern involving a child or young person, please contact 01344 352020

Vulnerable Adults

To discuss an e-safety concern involving a vulnerable adult, please contact Adult Social Care and Health Community Response and Re-enablement Team on 01344 351500

For professional advice, contact the UK Safer Internet Centre's Helpline on helpline@saferinternet.org.uk or 0844 381 4772.

To request an e-safety presentation for parents/carers or for children, young people and vulnerable adults, please contact Childnet on kidsmart@childnet.com or Microsoft on stuartha@microsoft.com.

This policy to be read in conjunction with:

- Safeguarding Policy
- Positive Behaviour Policy

APPENDIX A – E Safety Rules (Younger Children)

E-safety Rules

- Ask permission before using the internet
- Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details
- Make sure that when using social networking sites, privacy settings are checked regularly so that not just anyone can see your page/photos.
- The majority of social networking sites are not available to people under 13 years of age, so always seek permission from an adult before joining one
- Only contact people that you have actually met in the real world
- Never arrange to meet someone that you have only met on the internet
- Think very carefully about any pictures that you post online or contacting people via video (facetime, skype, webcam)
- Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult
- Only open e-mails, messages or web links from people that you know
- Avoid using websites that you wouldn't tell anyone about

Immediately minimise or walk away from anything on your screen that you are uncomfortable with and tell a trusted adult if you see anything that makes you feel unsure.

Never let people say nasty things to you on the internet. If they do:

- Tell the website
- Do not delete the nasty things they said
- Do not speak to them anymore
- Do not say nasty things back to them
- Tell someone you trust

APPENDIX A – E Safety Rules (Younger Children)

Early Years/KS1 Pupil Acceptable Use in School Agreement

- I will ask permission before using the internet
- I will not give out any personal information such as name, address, telephone number(s), age, school name or bank card details
- I will immediately close or walk away from anything on your screen that I am uncomfortable with and tell a trusted adult if I see anything that makes me feel unsure.
- I will make sure that when using social networking sites, privacy settings are checked regularly so that not just anyone can see your page/photos.
- I will only contact people that you have actually met in the real world
- I will never arrange to meet someone that you have only met on the internet
- I will think very carefully about any pictures that I post online or contacting people via video (facetime, skype, webcam, snapchat)
- I will never be mean or nasty to anyone on the internet or when using a mobile phone.
- If I know of someone being mean to another person, I will tell a trusted adult
- I will only open e-mails, messages or web links from people that I know
- I will avoid using websites that I wouldn't tell anyone about

Signed by Parent:……

On behalf of:

Child Name:…….

Year Group:…….

APPENDIX B – St Edward's Catholic First School Catholic School

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers with permission from a member of staff.
- I will ensure that I handle the school's computer with care.
- I will keep my logins and passwords secret.
- I will not bring a USB into school.
- If I have permission to bring a digital device into school, I will keep it in the school office.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult.

Child to Sign…… Class ……

Print Name……..

I have discussed these rules with my child and they understand what is expected from them and know what to do when there is an issue.

Parent to Sign…… Date……

Print Name……..

APPENDIX C – Internet Safety Tips and Tricks for Parents / Carers

Internet Safety Tips and Tricks

It is important for carers to remind any child/young person who uses the internet or other communication technology of the following:

- Always explore the privacy settings of your social networking site to protect your privacy and to protect yourself from strangers (for a range of online tutorials, go to https://www.childnet.com/resources/looking-for-kidsmart/) Facebook users can download a CEOP application to their Facebook page at http://apps.facebook.com/clickceop which enables quick access to help at a touch of a button
- Get friends and family to have a look at your social networking site to check that you aren't giving out too much personal information or posting inappropriate photos/films. They might see something you've missed
- Keep your passwords to yourself
- Respect yourself and others online
- If you are unlucky enough to have a bad experience, online report it to the service provider and tell a trusted person. You can also report to: or phone 101 (police non-emergency number)
- Cyberbullying is never acceptable.

If you or someone you know is targeted by bullies online, tell them to:

report the bully to the website/service operator

- keep evidence of the bullying behaviour
- resist the temptation to reply to nasty messages
- tell a trusted person

For more advice and tips, go to:
https://rbwmsafeguardingpartnership.org.uk/p/safeguarding-children/keeping-safe-online

Appendix D – Be Safe when using the Internet Children

Be safe when using the Internet

Ask someone you trust to make sure you are safe on the internet and Facebook (find out more at https://www.childnet.com/resources/looking-for-kidsmart/).

Never tell anyone anything about you on the internet.
Never show them pictures. Tell someone you trust what you talked about on the internet.

Never tell anyone your passwords.
Be nice to others online.
If someone is nasty to you on the internet, tell someone who looks after you.
Phone 101 to tell the police, or www.ceop.police.uk

Never let people say nasty things to you on the internet. If they are:

- Tell the website
- Do not delete the nasty things they said
- Do not speak to them anymore
- Do not say nasty things to them
- Tell someone you trust

APPENDIX E – ACCEPTABLE USE POLICY

Use of Digital Technology in St Edward's Catholic First School

This covers the use of digital technologies in the organisation, i.e. email; internet; intranet & network systems; learning platforms; software; mobile technologies; all equipment and systems. Any questions you may have regarding e-safety or the acceptable use of the ICT facilities in the school should be directed to .

By signing this form, you agree to the following:

Using the ICT Facilities in or provided by the school

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the senior leadership team or ICT Subject Leader
- I will ensure that any hardware, such as laptops, given to me are always brought to school to ensure effective teaching and learning
- I will ensure that teachers laptops are not left in a vulnerable place in a vehicle. Laptops must never be left in vehicles overnight
- I have signed the laptop registration form annually and I understand that I will not loan my laptop for an extended period of time to a colleague or to anyone else including family members
- I will only use the school-based email address for correspondence with colleagues, other professionals, parents or carers. I will not use any personal email addresses for any business associated with school
- I will ensure that all login details, including usernames and passwords, remain confidential to me. I will not share these details with anyone or permit anyone to use these
- I will ensure that I do not share the pupils' login details for online platforms (e.g., SPAG.com, Timetable Rockstars, etc.) or compromise this information in any way.
- I will ensure that I set appropriate work for the pupils in my class on online platforms (e.g., Mathletics, SPAG.com, Timetable Rockstars, Evidence Me etc.) in accordance with the national curriculum and, if necessary, adapt this accordingly for pupils who require this e.g., SEND
- I will ensure that screens are locked using CTRL-ALT-DEL if I leave the laptop or monitor
- I will not connect a computer, laptop, tablet or other device to the network without approval from the ICT lead and/or Executive Headteacher and Head of School
- I will not allow unauthorised individuals to access email, internet or school network.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed. If I require software for a legitimate purpose, I will contact the ICT technician who will provide me with advice

- I understand that all internet and network usage can be logged, and this information could be made available to the Executive Headteacher and Head of School/line manager on request.

Safeguarding Pupils

- I will follow the 'Guidance for Safer Working Practice for Adults who work with Children and Young People'
  I will not use personal digital cameras or the camera facility on mobile phones to take pictures or transfer images of pupils, young people or staff
- Any data which includes pupil names with any other identifying factor (i.e. surname, date of birth, address) will only be kept on the school encrypted computers/laptops or encrypted memory disk
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the admin office who will liaise with the ICT technician to ensure the filters are updated
- I will ensure that my personal email accounts, mobile/home telephone numbers are not shared with pupils, young people or their families
- I will not browse, download or send material that could be considered offensive to colleagues or any individual
- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that I keep up to date with digital safeguarding issues, including e-safety, so that they are appropriately embedded in my practice. I know that I can contact the DSL for more information.

Use of Social Media

- I will not access any social networking sites during my working hours either using personal mobile phones/tablets or school ICT equipment
- I will not allow pupils or young people to add me as a friend to their social networking site/s nor will I add them as friends to my social networking site/s
- I will ensure that any social networking sites or blogs that I create or actively contribute to are not confused with the role that I am employed to undertake.
- I will not use these forums to make any comments or post photographs in relation to the school, colleagues or pupils
- I will not share information about the school or make comments about school on any social networking site or internet forum. I understand that this is unacceptable behaviour and can bring the school into disrepute and may place pupils or staff at risk
- I understand that I have a responsibility to alert the Executive Headteacher and Head of School if I see or become aware of inappropriate information about staff or pupils through social media sites
- I will not have my personal social media devices (mobile/ tablet) in class.
- I understand that the Data Protection Act requires that any information seen by me with regard to staff, pupils or young people, held within our

organisation systems, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I understand that failure to comply with this Acceptable Use Policy will lead to disciplinary action.

Staff Signature

· I agree to comply with the statements above – The Acceptable Use Policy

· I understand that it is my responsibility to remain up-to-date with e-safety procedures for staff and pupils.

Signature: …… Date: ……

Full Name: ……Job Title: - …….

Manager Confirmation

I can confirm that this employee can be established on the email and network systems in the school, where applicable.

Signature……..Date: ……

Full Name……Job Title: ……

Appendix F – LAPTOP RESPONSIBILITY CONTRACT AND CONSENT

Laptop Responsibility Contract and Consent

Staff Name:……..

Laptop Make:_____ Laptop Number:_____

I acknowledge receiving a laptop computer for school use while I remain in the employment of St Edward's Catholic First School. I have read the attached Acceptable Usage Policy. In order to maintain this privilege, I agree to the following responsibilities:

(Staff initial each line please)

_____I agree to keep this laptop computer in my possession at all times. I will not give
or lend it to anyone except to return it to the school for upgrades, network connection
or repair in case it is damaged.

_____I agree to carry this laptop in a padded case or backpack (where provided), to minimise the chances that it will be damaged or destroyed.

_____I agree to read and follow the school's Acceptable Usage Policy (see next page),
and will not use this laptop, in or out of school, for inappropriate or unlawful purposes.

_____I agree to turn in my laptop to the school whenever requested for occasional maintenance, updates, or repairs.

_____I understand that if my laptop is lost or stolen, I will immediately notify the School and the police to obtain a crime number.

_____I agree to return this laptop to the school before I leave St Edward's Catholic First School Catholic
Primary School.

_____I understand that failure to comply with any of these rules and policies will result
in the suspension of my use of this laptop. Restoration of this privilege may require the
involvement of the Executive Headteacher and Head of School.

Staff Signature:…….. Date:……

Print Name:……..

Checked by ICT Co-ordinator:……

SOFTWARE

Only licensed software may be installed onto school laptops & computers.

Software currently installed on the laptop computer includes the following: •

- Microsoft 365
- Microsoft Internet Explorer & Google
- Microsoft Suite

Teachers are not authorised to install unlicensed software on computers. If a teacher
requires special or non-standard software to be installed on laptops for school use, it must be cleared by the Executive Headteacher and Head of School/ICT Co-ordinator. The teacher will be responsible
for supplying licenses, media, and any documentation. Licence information is a requirement of the Auditors.

Breach of these conditions may lead to disciplinary action.

1. The user shall not in any way, tamper or misuse school equipment, either

software or hardware. No form of tampering is acceptable.

2. Laptops can have access to the Internet. Abuse of this access, in the form of

access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious breach of the law (Child Trafficking and Pornography Act 1998). The school will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.

3. E-mail and Internet chat rooms, where these relate to their Schoolwork or study, should be used in a courteous manner, respecting the etiquette of the network. Usage of any form of profanity in these communications is absolutely forbidden.
4. Users may not download copyrighted software, audio or video files, or any other copyrighted material from the Internet. Any such material found will be deleted without prior notification.

5. Software in use in the school is licensed in a correct and legal manner. Users should make no attempt to copy licensed or copyrighted material from the School network.

6. E-Mail should be considered as an insecure medium for the transmission of

confidential information. Where confidential information is to be transferred, externally, it should be done in an encrypted form.

7. Notwithstanding that every effort is made to ensure that home folders and e-

mail are secure, the School does not in any way guarantee the security of this data.

8. Food and drinks should be kept well away from laptops. The user should also take care when shutting down and closing the lid of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case the user will be liable for repair costs.

Guidelines for User Responsibilities

Use of St Edward's Catholic First School ICT resources is granted based on acceptance of the following specific responsibilities:

Use only those computing and information technology resources for which you have authorisation. For example: it is a violation:

- to use resources, you have not been specifically authorised to use
- to use someone else's account and password or share your account and password with someone else
- to access files, data or processes without authorisation
- to purposely look for or exploit security flaws to gain system or data access

Use computing and information technology resources only for their intended purpose.
For example: it is a violation:

- to send forged email
- to misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with other systems or users
- to use electronic resources for harassment or stalking other individuals
- to send bomb threats or "hoax messages"
- to send chain letters
- to intercept or monitor any network communications not intended for you
- to use computing or network resources for advertising or other commercial purposes
- to attempt to circumvent security mechanisms

Protect the access and integrity of computing and information technology resources.
For example: it is a violation:

- to release a virus or worm that damages or harms a system or network
- to prevent others from accessing an authorised service
- to send email bombs that may cause problems and disrupt service for other users
- to attempt to deliberately degrade performance or deny service
- to corrupt or misuse information
- to alter or destroy information without authorisation

Abide by applicable laws and university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
For example: it is a violation:

- to make more copies of licensed software than the license allows
- to download, use or distribute pirated software
- to operate or participate in pyramid schemes
- to distribute pornography to minors
- to upload, download, distribute or possess child pornography

Respect the privacy and personal rights of others. For example: it is a violation:

- to tap a phone line or run a network sniffer without authorisation
- to access or attempt to access another individual's password or data without explicit authorisation
- to access or copy another user's electronic mail, data, programs, or other files without permission

APPENDIX G - Inappropriate and Illegal Online Acts

Inappropriate and Illegal Online Acts

Children, young people, vulnerable adults as well as organisation staff and volunteers who work with them must be aware of what is considered to be criminal when using the internet and electronic communication technologies. This should be reflected in the AUPs and education programmes delivered on an ongoing basis. While the list below is not exhaustive, it is hoped to provide some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

It is noted that all incident types below are considered criminal in nature but would be subject a full investigation in order to determine whether a crime has been committed or not.

Copyright infringement through copying diagrams, texts and photos without acknowledging the source

- Misuse of logins (using someone else's login)
- Distributing, printing or viewing information on the following:
    - Soft-core pornography
    - Hate material
    - Drugs
    - Weapons
    - Violence
    - Racism
- Distributing viruses
- Hacking sites
- Gambling
- Accessing age restricted material
- Bullying of anyone
- Viewing, production, distribution and possession of indecent images of children(1)
- Grooming and harassment of a child or young person
- Viewing, production, distribution and possession of extreme pornographic images
- Buying or selling stolen goods
- Inciting religious hatred and acts of terrorism
- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above)(2)

(1) Where the victim is under the age of 18 (recently changed from 16 years old by Section 1 of the Protection of Children Act 1988, as amended by the Criminal Justice and Public Order Act 1994 and Schedule 6 of the Sexual Offences Act 2003) and where the offender has attained the age of 10 (criminal age of responsibility). It is noted that the viewing of information of this nature may, in some circumstances, be appropriate i.e. research on hate crime, drugs etc. (2) Compiled in consultation with Thames Valley Police and SEGfL

APPENDIX H – Legal Framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice and organisations should always consult with their legal team or the police.

Many young people and indeed some organisation staff and volunteers use the internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison. The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Schools should have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (e.g. using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (e.g. caused by viruses or denial of service attacks). UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will

allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Executive Headteachers and Head of Schools have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy (please see Appendix J for a more detailed template/policy).

APPENDIX I - Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)

Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)

- If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed, often works.
- Failing that, having kept a copy of the page or message in question, delete the content.
- For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.
- For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column. Always try to cite which of the Facebook Terms and Conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or Community Standards at http://www.facebook.com/communitystandards/. Note that Facebook are more alert to US law than UK. The process should be anonymous.
  If the page is by someone under 13 click on https://www.facebook.com/help/157793540954833/?helpref=uf_share (Facebook say they will delete any such page).
- To remove a post from a profile, hover over it and on the right there will be a cross to delete it.
- Does the incident trigger the need to inform the police or child protection agencies?
- To report abuse or harassment, email abuse@facebook.com (Facebook will acknowledge receipt of you email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint).
  If all else fails, support the victim, if they wish, to click the 'Click CEOP' button http://www.thinkuknow.co.uk/
  If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be done here
  https://ssl.facebook.com/help/contact.php?show_form=delete_account They should be made aware of the privacy issues that might have given rise to their problem in the first place:
- You will not bully, intimidate, or harass any user (1.3.6)
- You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission (4.1)
- You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law (5.1)

NOTE: An effective education programme can help to reduce the number of times that this sort of incident arises, over the medium term. Such a programme should help young people to match their online behaviour with their offline behaviour by helping them to develop understanding, skills and behaviours in these sorts of areas:

- possible consequences
- understanding the effects of bullying on others
- understanding how technology can magnify impact
- understanding how comments or other actions can be perceived differently by the originator and the target

APPENDIX J - Electronic Devices –Searching & Deletion

Electronic Devices -Searching & Deletion

With the ever-changing face of information technology and the increasing use of such by pupils there have had to be amendments to the Education Act 2011 (Part 2). These changes have afforded schools powers (by statute) to search pupils to maintain safety and ensure discipline. Whilst we must accept that there are no guarantees that the school will not face a legal challenge, the Governors of St Edward's Catholic First School believe that by having robust policies in place we will be able to provide sufficient justification for what actions the school may take to ensure the above.

This appendix deals with the power to search pupils for items banned under the 'school rules' and the power to 'delete data' stored on seized electronic devices, i.e. mobile phones, IPads, notepads, etc. which have been used inappropriately on school premises. (Pupils only)

The new act allows for an authorised person, in the case of St Edward's Catholic First School the Executive Headteacher and Head of School, to examine data on any electronic device brought onto the school premises if there is good reason to believe that any such data may be used to cause harm, disrupt teaching or break any the school's rules. Following examination, if there is good reason to do so the data may be removed – the device can then be returned to the owner, retained or disposed of. Details of this policy for searching will also be included in the Behaviour /Positive Relationships Policy.

The Executive Headteacher and Head of School is responsible for ensuring the school policies reflect the requirements contained in the relevant legislation.

Whilst it may be necessary to delegate the responsibility of a searching to another designated member of staff, where ever possible it should only be carried out by the Executive Headteacher and Head of School. Any other member of staff delegated this task must be fully aware of the school's policy on devices brought into school and the rules on 'deletion' and have received any appropriate training in order to judge whether material is inappropriate or illegal.

Behaviour

If pupils breach the rules on what is allowed to be brought into school the sanctions contained in the Positive Relationships Policy will be used. See Positive Relationships Policy.

Carrying Out a Search

The Executive Headteacher and Head of School, or delegated member of staff, must have reasonable grounds for suspecting that a pupil is in possession of an item banned under the school rules and which can be searched for. The person carrying

out the search must be of the same gender as the pupil involved and there MUST be another witness present (also a member of staff) if at all possible again the same gender of the pupil involved. There are very limited exceptions to this rule. Authorised staff can search a pupil of the opposite gender including without a witness present, but only where they reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search

The person carrying out the search may not require the pupil to remove any other clothing other than outer clothing, i.e. clothing not worn next to the skin, or covering underwear (outer clothing includes, hats, gloves, coats, blazers, shoes, scarves).

Possessions can only be searched in the presence of the pupil and another member of staff except where there is a risk of serious harm being caused to a person if the search is not conducted immediately and when it is not practicable to summons another member of staff. Possessions means any good over which the pupil has or appears to have control including desks, lockers and bags.

Use of Force - Force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say the item can be searched for.

Electronic Devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material

- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. Care will be taken not to delete material that might be required in a potential criminal investigation.

The school will also consider our duty of care responsibility in relation to those staff that may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting.

Deletion of Data

Following an examination of an electronic device, if the Executive Headteacher and Head of School has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. they must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the Executive Headteacher and Head of School to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Audit / Monitoring / Reporting / Review

The responsible person, Executive Headteacher and Head of School, will ensure that full records are kept of incidents
involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the E Safety Governor and the E Safety Officer annually.

This policy will be reviewed by the Executive Headteacher and Head of School and governors annually and in response to changes in guidance and evidence gained from the records.

The school's policies on Positive Relationships and E Safety are available on request or via the school web site.

APPENDIX K – Further Guidance

CEOP (Child Exploitation and Online Protection Centre)

http://www.ceop.gov.uk

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. That means that they are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

Think U Know

http://www.thinkuknow.co.uk

Think U Know is CEOP's support, guidance and resource site for children, young people, parents, carers and adults who work with children and young people.

UK Safer Internet Centre

http://www.saferinternet.org.uk/

This website provides the latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focusing on the safe and responsible use of the internet and new technologies.

Childnet

http://www.childnet-int.org

Childnet is a non-profit organisation working with others to "help make the Internet a great and safe place for children". The website gives news and background to Childnet's work and serves as a portal to Childnet's award-winning projects.

Teach Today

https://www.teachtoday.de/en/

Teachtoday provides information and advice for teachers, Executive Headteacher and Head of Schools, governors and other members of the school workforce about the positive, responsible and safe use of new technologies. The above link provides advice and guidance on cyberbullying towards teaching staff.

NASUWT: The Teachers' Union

https://www.nasuwt.org.uk/advice/health-safety/social-media-and-online-abuse-of-teachers.html

The NASUWT is the largest teachers' union in the UK. The NASUWT is the only TUC-affiliated teachers' union to represent teachers in England, Northern Ireland, Scotland and Wales. NASUWT organises in all sectors from early years to further education and represents teachers in all roles including heads and deputies.

NASUWT is politically independent and is deeply committed to working to influence the education policy of the Government and employers. The above link provides guidance and support on the subject of cyberbullying towards teaching staff.

APPENDIX L – PHOTOGRAPHY POLICY

The Photography Policy sets out to ensure that:

- Photographs are only used for the purpose intended;
- School use of photographs is facilitated;
- Personal family photography is allowed where possible;
- Parents and pupils are given the opportunity to opt out.
- Individual rights are respected and child protection ensured;

Throughout this policy, 'photography' refers to digital images, videos and photographic prints or slides. 'In school' refers to all occasions, whenever and wherever pupils are the responsibility of the school staff. 'Parent' refers to anyone with parental rights and responsibilities in relation to a pupil.

POLICY AIM

The main rationale for this Policy is to strengthen the school's Child Protection procedures, to ensure that all of our children, including the most vulnerable, remain safe while in school and taking part in school activities. With the increasing risk posed to vulnerable individuals by the development of social networking groups and other Internet sites, it has been considered necessary to review how images of children are shared with, and by, parents and the school. We, also, acknowledge the need to be mindful of Copyright in Performance restrictions.

This policy will be reviewed regularly by the Governing Body within the agreed cycle of Policy Review.

During the school year, there are a number of occasions when school staff or parents will want to take photographs of pupils. Such occasions include everything from assessment and curricular purposes in the classroom to awards ceremonies, school productions and sporting events, as part of the wider life of the school.

PARENTAL ACCESS TO PHOTOGRAPHY

Parents and Carers should take account of the "Use of Camera and Video Code"

Use of Media Code: A guide for parents who wish to use photography and / or video at a school event.

See Appendix M – Use of Media Code

Generally, photographs and videos for school and family use are a source of innocent pleasure and pride, which can enhance self-esteem for children and young people and their families. We must, however, pay attention to child protection issues and safety requirements and balance the rights of individual children's privacy with the rights of parents to record their children's achievements.

Remember that parents and carers attend school events at the invitation of the Executive Headteacher and Head of School and Governors.

The Executive Headteacher and Head of School and Governors have the responsibility to decide the conditions that will apply, in order that children are kept safe and that the performance is not disrupted, and children and staff are not distracted.

We recognise that parents and carers and family members wish to record events such as school plays, sports days etc. to celebrate their child's achievements. St Edward's Catholic First School is happy to allow this on the understanding that such images/recordings are used purely for family purposes.

Parents and Carers can use photographs of their own child taken at a school event for their own personal use only but should not share team photographs or photographs including other children. Such photographs cannot be sold and must not be put on the web/internet including social networking sites, due to existing Data Protection legislation.

Recording or photographing other than for private use would require the consent of all the other parents whose children may be included in the images.

Parents are asked to take guidance from the school staff regarding the timing and procedures for permitted photography.

Parents and carers must not photograph or video children changing for performances or events.

These, or any other, photographs of a child, other than a parent's own child, must not be uploaded onto the Internet, including Facebook or any other social interaction sites, without the express permission of the child's parent or carer.

Parents and Carers agree to these terms via Appendix M – Use of Media Code

SCHOOL USE OF PHOTOGRAPHS

The school uses photographs for a number of purposes:

- Assessment of pupils in some class situations;
- Illustrating aspects of learning and teaching;
- Recording events in the life of the school;
- Publicity - From time to time, the media are asked to cover school events. It is an important part of publicising pupil achievement and informing the public about educational initiatives;
- School Website - Photographs of pupil activities and achievements may be posted on the school website.
- Social Media – St Edward's Catholic First School Instagram page

It is taken that children attending St Edward's Catholic First School may have their picture taken unless the child(ren)s' parents inform the school in writing they cannot. Photographs will not be used to any purpose other than that originally intended.

Photographs will be stored electronically, only for as long as the purpose for which they were taken remains valid. Once that purpose expires, photographs will be deleted.

APPENDIX M – Use of Media Code

St Edward's Catholic First School Use Of Media Code

Generally, photographs and videos for school and family use are a source of innocent pleasure and pride, which can enhance self-esteem for children and young people and their families. We must, however, pay attention to child protection issues and safety requirements and balance the rights of individual children's privacy with the rights of parents to record their children's achievements.

Remember that parents and carers attend school events at the invitation of the Executive Headteacher and Head of School and Governors.

The Executive Headteacher and Head of School and Governors have the responsibility to decide the conditions that will apply, in order that children are kept safe and that the performance is not disrupted and children and staff are not distracted.

We recognise that parents and carers and family members wish to record events such as school plays, sports days etc. to celebrate their child's achievements. St Edward's Catholic First School is happy to allow this on the understanding that such images/recordings are used purely for family purposes.

Parents and Carers can use photographs of their own child taken at a school event for their own personal use only but should not share team photographs or photographs including other children. Such photographs cannot be sold and must not be put on the web/internet including social networking sites, due to existing Data Protection legislation.

Recording or photographing other than for private use would require the consent of all the other parents whose children may be included in the images.

Parents are asked to take guidance from the school staff regarding the timing and procedures for permitted photography. Parents and carers must not photograph or video children changing for performances or events.

These, or any other, photographs of a child, other than a parent's own child, must not be uploaded onto the Internet, including Facebook or any other social interaction sites, without the express permission of the child's parent or carer.

Parents and Carers agree to these terms via the permission slip below.
Please complete, detach and return the slip to the school office.

I AGREE TO THE TERMS OF THE USE OF CAMERA AND VIDEO CODE

Child/ren Name/s: ……Year Group/s: ……
Parent/Carer Name: …… Signature: …… Date:……..

Parent/Carer Name: …… Signature: …… Date:……..