E-SAFETY POLICY AND GUIDANCE

MISSION STATEMENT

We are growing together on our journey of achievement with Jesus in our hearts, heads and hands.

POLICY STATEMENT

The Governors of St Joseph's Primary 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.

The government has published a new guidance document 'Teaching online safety in school (DfE, June 2019) https://www.gov.uk/government/publications/teaching-online-safety-in-schools

This outlines the importance of helping children and young people not only use the internet safely, but also give them opportunities to learn how to behave online. Throughout, the guidance emphasises the importance of teaching that is always age and developmentally appropriate.

It is the responsibility of the Governors and Senior Leadership Team (SLT) of St Joseph's 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 Joseph's Primary 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 Bracknell Forest Community Safety Partnership's (CSP's) e-safety Strategy and Action Plan (http://www.bracknell-forest.gov.uk/esafety), the Pan Berkshire Local Safeguarding Children Board Child Protection Procedures (http://proceduresonline.com/berks/) and the Berkshire Safeguarding Adults Policy and Procedures
https://www.berkshiresafeguardingadults.co.uk/bracknell/

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 such as Xbox, PlayStation, Nintendo switch and Wii.

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 are able to 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 the 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 have the opportunity to 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, focus 'days', and P4C in addition to weekly 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 will also invite parents to attend a workshop bi-annually. Each class will display a poster to remind pupils about keeping safe
https://www.childnet.com/resources/a3-posters-to-download

St Joseph's school recognises 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.
Teaching online safety at St. Joseph's School will be in conjunction with Education for a Connected World Framework (UKCIS, 2018) which offers 'age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.'

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 ever-changing as technologies develop. These can be summarised as the 5Cs

Content

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

Communication

- Commercial (tracking, harvesting personal information
- Aggressive (being bullied, harassed or stalked)
- Sexual (meeting strangers, being groomed)
- Values (self-harm, unwelcome persuasions)

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)

- Aggressive (bullying or harassing another)
- Sexual (creating and uploading inappropriate material)
- Values (providing 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 Joseph's 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 be the Deputy Head Teacher with the support of the Senior Leadership Team, who 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 also be the Safeguarding designated Governor.
The responsibilities of the e-safety lead will be:-

- Maintaining the AUPs alongside SBM
- Attend CEOP training
- 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
- Monitor pupil usage on a half termly basis using Securus
- Lead a whole school assembly each term

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.
A flow chart and policy is available in Staff Room on Safeguarding board.
E safety lead to monitor internet use using 'Securus'

Has there been inappropriate contact?

1. Report to the organisation manager/e-safety lead/child protection officer
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

Has someone been bullied?

1. Report to the organisation manager/e-safety lead/child protection officer
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/child protection officer
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/child protection officer
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 2011 should be referred to (http://berksadultsg.proceduresonline.com/index.htm).

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 is 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.

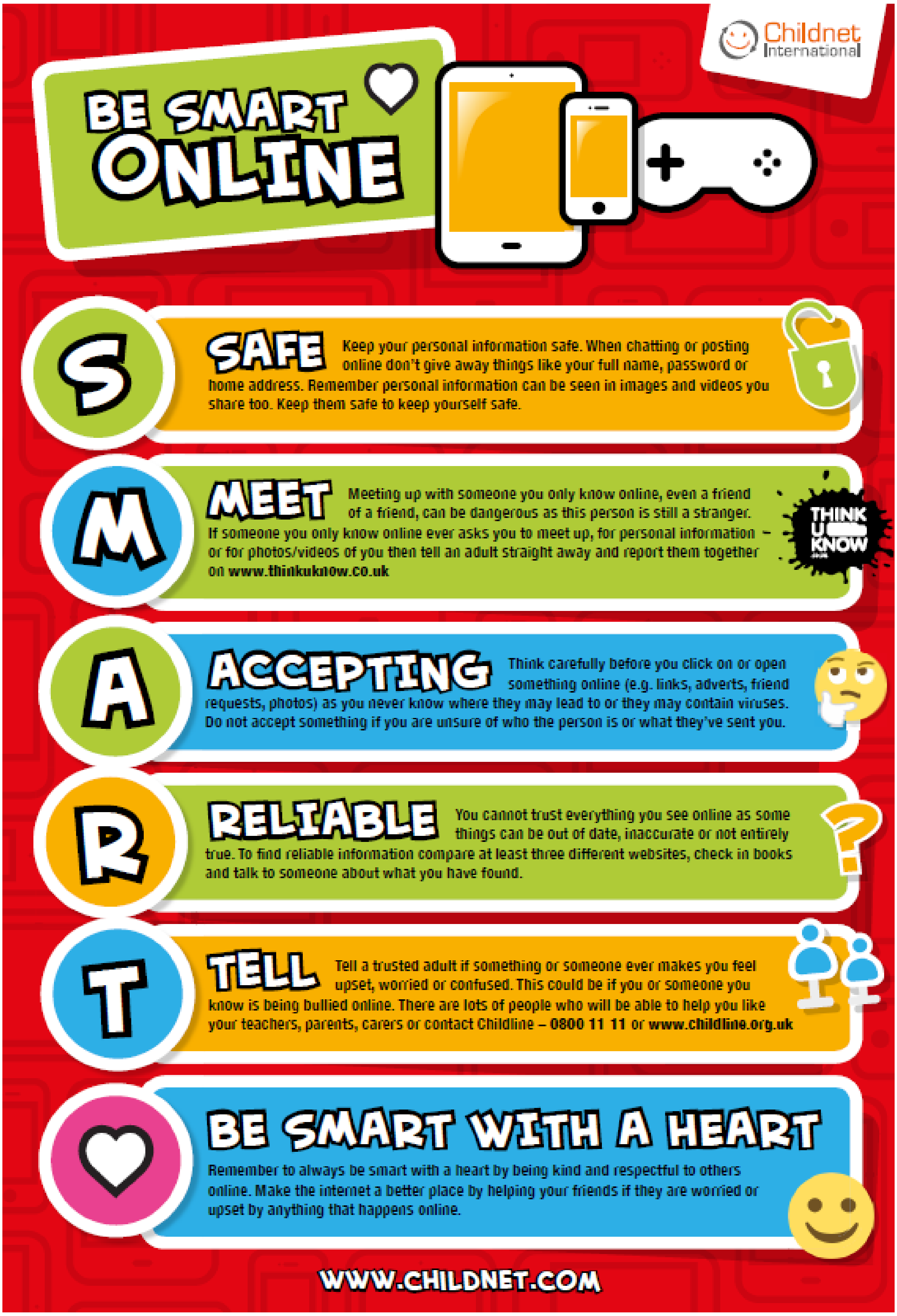
To request to attend e-safety workforce training, please contact Liz Challis at Bracknell Forest Council on 01344-352000.

This policy to be read in conjunction with:
Safeguarding Policy

Positive Relationships (Behaviour) Policy
Teaching and Learning Policy
ICT Policy
Policy reviewed by N Philpott November 2019
Policy to be reviewed annually.

Approved by the Governing Body	/ /
Chair of Governors signature Date	…………………………………………………… / /
Review date	/

APPENDIX A – E Safety Rules (All Children)



Childnet International
THINK U KNOW

BE SMART ONLINE

S **SAFE** Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M **MEET** Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

A **ACCEPTING** Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R **RELIABLE** You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T **TELL** Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**

BE SMART WITH A HEART Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

WWW.CHILDNET.COM

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.

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 and use a student friendly search engine such as http://www.askforkids.com

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 you 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 and use a student friendly search engine such as http://www.askforkids.com

APPENDIX B – St. Joseph's 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 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 ………………

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………………

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 http://www.kidsmart.org.uk/skills-school/)
- 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: CEOP REPORT ceop.police.uk 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:
http://www.bracknell-forest.gov.uk/esafety

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 http://www.kidsmart.org.uk/skills-school/).

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

For more tips, go to:
http://www.bracknell-forest.gov.uk/esafety

SOFTWARE

Only licensed software may be installed onto school laptops & computers.
Software currently installed on the laptop computer includes the following:

- Microsoft Internet Explorer
- Microsoft Word
- Microsoft Power Point
- Microsoft Excel
- Easiteach

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 ICT Co-ordinator/ICT Systems Manager beforehand. The teacher will be responsible for supplying licenses, media, and any documentation. Licence information is a requirement of the LA 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, in particular 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. Joseph’s Catholic Primary 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 E - 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 F – Legal Framework

Legal Framework

Notes on the 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:

- Headteachers 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 G - Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)

Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)

1. 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.

2. Failing that, having kept a copy of the page or message in question, delete the content.

3. For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.

4. 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.

5. If the page is by someone under 13 click on http://www.facebook.com/help/contact.php?show_form=underage (Facebook say they will delete any such page).

6. To remove a post from a profile, hover over it and on the right there will be a cross to delete it.

7. Does the incident trigger the need to inform the police or child protection agencies?

8. 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).

9. If all else fails, support the victim, if they wish, to click the 'Click CEOP' button http://www.thinkuknow.co.uk/

CEOP REPORT
ceop.police.uk

10. 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 H –

PHOTOGRAPHY POLICY

MISSION STATEMENT

We are growing together on our journey of achievement with Jesus in our hearts, heads and hands.

POLICY STATEMENT

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;
- Individual rights are respected and child protection ensured;
- Parents and pupils are given the opportunity to opt out.

Throughout this policy, 'photography' refers to digital images, DVD's, 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.

1. 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 A – 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 Head teacher and Governors.

The Head teacher 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 Joseph's 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 photograph permission form attached.

2. 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 Joseph's Twitter page (@stjosephsbrack)

The school will always obtain the permission of the parent or carer if images are used of children in any of the above. The attached form will allow parents to inform us if they do not wish their children to be photographed for press and publicity purposes. Photographs will not be used to any purpose other than that originally intended. Photographs will be stored electronically, (office 365) only for as long as the purpose for which they were taken remains valid. Once that purpose expires, photographs will be deleted.

ST JOSEPH'S CATHLOLIC PRIMARY 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 Head teacher and Governors.

The Head teacher 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 Joseph's 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: ……………………………………………………………………

Parent/Carer Signature: ………………………………………………………………

Date: ………………………………………………………………………………………..

APPENDIX I - Electronic Devices – Searching & Deletion

Electronic Devices - Searching & Deletion

Introduction

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 in order 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 Joseph's 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.

List items which would be banned i.e. mobiles phones, IPod's, notepads etc. (Pupils only)

The new act allows for an authorised person, in the case of St Joseph's, the Headteacher, 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 schools 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 Headteacher 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 Headteacher. 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 Headteacher, 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.
Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart – http://www.swgfl.org.uk/safety/default.asp. Local authorities / LSCBs may also have further guidance, specific to their area.

Deletion of Data

Following an examination of an electronic device, if the headteacher 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 headteacher 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, Headteacher, 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 headteacher and governors annually and in response to changes in guidance and evidence gained from the records.

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

Appendix J

St. Joseph's Catholic Primary School, RG12 9AP Technology Acceptable Use Agreement – Staff

Whilst our school promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully and sign below to show you agree to the terms outlined.

1. Using technology in school

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information or for any work purposes.
- I will not share sensitive personal data with any other pupils, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the headteacher.
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a regular basis.
- I will only use recommended removable media and will keep this securely stored in line with the GDPR.

- I will only store data on removable media or other technological devices that has been encrypted of pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary and which is encrypted.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.
- I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the headteacher.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the IT technican to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the headteacher before accessing the site.

- I will not communicate with pupils or parents over personal social networking sites.
- I will not communicate with parents over personal social networking sites, unless permission has been given by the headteacher.
- I will not accept 'friend requests' from any pupils over personal social networking sites.
- I will not accept 'friend requests' from any parents over personal social networking sites, unless permission has been given by the headteacher.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.
- If staff are parents, the headteacher should be made aware of any social media used with other parents of the school. Be viligent and do not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.

4. Working at home

- I will adhere to the principles of the GDPR when taking work home.
- I will ensure I obtain permission from the headteacher /data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the DPO and IT technician before it is used for lone-working.

- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will act in accordance with the school's E-Security Policy when transporting school equipment and data.
- I will not use any unsecured Wireless networks and will be aware of the potential risk to personal data when working in public space, ensuring that such data is not visible to other or laptops left open when I am away from the device.

5. Training

- I will ensure I participate in any e-safety or online training offered to me and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Headteacher/ DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the E-Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the headteacher.
- I understand that my use of the internet will be monitored by the Leadership Team and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

7. Device Responsibility

- Staff will have an individually assigned laptop and/or iPad which will be theirs for the duration of their employment teaching a class.
- Staff should:
  - Bring the device (s) to school every day, fully charged.
  - Keep the device(s) with them or in a secured (locked) area at all times.
  - Return the device(s) to the school whenever requested for occasional maintenance, updates, or repairs.

    - Immediately report to the Headteacher any loss, theft or damage to the device(s)
    - Remember that the device(s) are for educational purposes.
    - Keep away from food or drink
- Staff should not:
    - Attempt to modify the device(s) hardware or operating system in any way.
    - Apply any permanent marks, decorations or modifications to the device(s)
    - Remove the school-supplied case.
    - Swap, give or lend the device(s) with another member of staff except to return it to the school for upgrades, network connection or repair in case it is damaged.
    - Dispose of or sell the device(s).
    - Add or remove applications from the device(s)
    - Change any configuration settings on the device(s), particularly network configuration.
- Staff agree that failure to comply with any of these rules and policies will result in the suspension of their use of the device(s). Restoration of this privilege may require the involvement of the Headteacher.

Staff User Agreement Acceptance Form

Staff name: ________________________________

Laptop Make: ________________________________ Asset No.__________________

iPad Model: ________________________________ Asset No.___________________

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed: Date:

Print name:

Signed headteacher: Date:

Print name:

DEVICE(S) RETURN

Device: ________________________________

Asset No.: ________________________________

Date of return ________________________________

Reason for return ________________________________

Staff member signature ________________________________

Receiving staff member signature ________________________________

Re-allocated location for device ________________________________

Device: ________________________________

Asset No.: ____

Date of return ____

Reason for return ____

Staff member signature ____

Receiving staff member signature ____

Re-allocated location for device ____