Social Media

1 INTRODUCTION

1.1 The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and *Instagram* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

1.2 Whilst recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that St Mary's School staff and contractors are expected to follow when using social media.

1.3 It is crucial that pupils, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school, the diocese and East Sussex County Council are safeguarded.

1.4 Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

2 SCOPE

2.1 This policy applies to St Mary's School Governing Body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this policy.

2.2 This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school

2.3 This policy applies to personal web space such as social networking sites (for example *Facebook*, *Instagram*), blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia*, social bookmarking sites such as *del.icio.us* and content sharing sites such as *Flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

3 LEGAL FRAMEWORK

3.1 St Mary's School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality,
- General Data Protection Regulations 2018

3.2 Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

3.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

3.4 St Mary's School and the County Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render St Mary's School or the County Council liable to the injured party.

4 RELATED POLICIES

4.1 This policy should be read in conjunction with the following school and County Council policies:

- East Sussex County Council Code of Conduct for Employees
- Safeguarding and Child Protection Policy
- Guidance for Safer Working Practice for Adults who Work with Children and Young People'.
- Government guidelines on the Prevent Duty through the Prevention of Extremism and Radicalisation Policy
- St Mary's School Mission Statement
- Data Protection Policy
- Privacy Notice

5 PRINCIPLES – *BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL*

5.1 You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school or County Council and your personal interests.

5.2 You must not engage in activities involving social media which might bring St Mary's School, the diocese or the County Council into disrepute.

5.3 You must not represent your personal views as those of St Mary's School, the Diocese or the County Council on any social medium.

5.4 You must not discuss personal information about pupils, St Mary's School, the Diocese or County Council staff and other professionals you interact with as part of your job on social media.

5.5 You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, St Mary's School, the Diocese or the County Council.

5.6 You must be accurate, fair and transparent when creating or altering online sources of information on behalf of St Mary's School, the Diocese or the County Council.

6 PERSONAL USE OF SOCIAL MEDIA

6.1 Staff members must not identify themselves as employees of St Mary's School or County Council or service providers for the school or County Council in their personal webspace. This is to prevent information on these sites from being linked with the school, the Diocese or the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

6.2 Staff members must not have contact through any personal social medium with any pupil, whether from St Mary's School or any other school, unless the pupils are family members.

6.3 St Mary's School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff

members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

6.4 Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

6.5 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites created according to the requirements specified in section 7 and Appendix A.

6.6 Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these in general terms in class.

6.7 On leaving St Mary's School's service, staff members must not contact St Mary's School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

6.8 Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, County Council staff and other parties and school or County Council corporate information must not be discussed on their personal webspace.

6.9 Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school or County Council uniforms or clothing with school or County Council logos or images identifying sensitive school, Diocesan or County Council premises (e.g. care homes, secure units) must not be published on personal web space.

6.10 School, Diocesan or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

6.11 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

6.12 St Mary's School, Diocesan or County Council corporate, service or team logos or brands must not be used or published on personal web space.

6.13 Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school's time.

6.14 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

6.15 Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

7 USING SOCIAL MEDIA ON BEHALF OF ST MARY'S SCHOOL

7.1 Staff members can only use official school sites for communicating with pupils, parents and carers or to enable these groups to communicate with one another.

7.2 There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.

7.3 Official school sites must be created only according to the requirements specified in Appendix A of this Policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

7.4 Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

7.5 Written permission from parents or carers must be obtained before photographs of or named photographs of students are published on the school's webspace.

8 MONITORING OF INTERNET USE

8.1 St Mary's School monitors usage of its internet and email services without prior notification or authorisation from users.

8.2 Users of St Mary's School email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's ICT system or hardware.

Acceptable Use

Introduction

All users of the school internet or school equipment are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the headteacher

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school, Church or County Council into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person. I will not reveal any of my personal information to students.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the ICT Subject Leader or technician.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username I will **not** continuing using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.

14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the DPOr.
15	I will not use phones, tablets or personal laptops on the network without having them approved by the school SLT
16	I will not use memory sticks or save data to 'Desktop' on school machines as this is not encrypted
17	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
18	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
19	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children.
20	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
21	I will support and promote the school's online safety and Data Protection policies and help students be safe and responsible in their use of the Internet and related technologies.
22	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held in SIMS.
23	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
24	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
25	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

Laptop and Removable Media Security

INTRODUCTION
St Mary's Catholic Primary School has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held and complies with the requirements of the Data Protection Act 1998. The use of portable computer devices increases the risks associated with the secure storage of data. The purpose of this policy is to set out the criteria for the conditions relating to the use of **School owned** laptop computers and data stored on **School-owned or Personal** removable media (e.g. flash drives/memory sticks, external hard drives).

For the purpose of this policy the term "laptop" is used to describe any portable computer device including laptops, notebooks, tablets, cameras, flash drives, on which school data may be stored. Your laptop is a valuable asset and an essential business tool. It needs to be protected, as does the information it stores. Remember that the laptop and the information that it contains could be valuable to thieves. By following the simple security measures listed below, you can help protect yourself and your laptop.

Staff Responsibilities
Members of staff must take personal responsibility for the security of the equipment, software and data in their care and abide by the following: (Please see glossary for definitions)

- If laptops must be left in cars, they must be stored out of sight (e.g. in covered boot). Laptops should never be left in a vehicle for prolonged periods of time or overnight.
- Unauthorised or unlicensed software must not be loaded on to the laptop.
- Ensure the laptop is not used by unauthorised persons.
- Take all reasonable steps to ensure that the laptop is not damaged through misuse.
- When travelling, laptops should not be left unattended in public places.
- Remain particularly vigilant when using your laptop and try to refrain from using it in public places (e.g. library, railway station).
- Return the laptop to school for regular health checks or when requested and ensure that the laptop antivirus software is updated by the school ICT technician.
- Ensuring that the protection settings are left as set up by the technician (E.g. that Windows Firewall always runs, passwords are in place).
- Passwords should be kept safe. Update your passwords regularly and don't let others use them.
- Return the laptop before leaving the employment of the school.
- Report any possible security breaches (e.g. laptop stolen or misplaced) to the DPO immediately.
- Ensure that the school office has noted any serial numbers for the equipment and asset tags have been created, where necessary.
- Do not allow family or friends to use your laptop, as there is a risk that school information could be compromised.

If you are attacked, never risk your own safety. Hand over the laptop. It can be always be replaced but you cannot.

School Responsibilities

It is the responsibility of the school to ensure the correct configuration of school-owned laptop devices. The staff member is responsible for ensuring the integrity of the configuration that had been set up by the school technician (e.g. not installing unauthorised software). The school will be responsible for:

- operating a "health check" programme. The configuration of the laptop will be checked, and any necessary software upgrades completed. The teacher must cooperate with the school and ensure that both school-owned and personal devices (which can carry viruses into the school system etc) are made available for checking.
- The school will keep a list of serial numbers for laptop devices and will notify the police if a school-owned device is stolen. The school will obtain a crime reference number and advise the school's insurers.
- The school will keep a list of help desk numbers/contact information (e.g. telephone numbers or website addresses to report thefts, cancel service and report faults).
- Ensure that the school's approved Anti-Virus software is installed (where appropriate) at the time of issue to staff. The anti-virus system must be updated on an annual basis. It is the responsibility of the teacher to

monitor this, and to contact the school ICT subject Leader or Technician if they believe this is not occurring. In no circumstances shall the user delete or disable the anti-virus software.

BREACHES OF THE POLICY

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with St Mary's School or County Council Disciplinary Policy and Procedure.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of St Mary's School or the County Council or any illegal acts or acts that render St Mary's School or the County Council liable to third parties may result in disciplinary action or dismissal.

Contracted providers of St Mary's School or County Council services must inform the relevant school or County Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

GLOSSARY

Authorised User:
A user who has been authorised to use the laptop, by being either the designated owner of the laptop, or a member of staff who has been given permission by the designated owner to use the laptop.

Unauthorised software:
This is software that has not been authorised for use or installation by the Head Teacher, ICT co-ordinator or ICT Technician.

Unlicensed software:
This is software for which the school or user does not possess a license (including downloads from the internet), and therefore has no legal entitlement to use. The use of such software would leave both the school and the individual open to legal action which could result in a heavy fine, or even imprisonment.

APPENDIX A

Requirements for creating social media sites on behalf of St Mary's Catholic Primary School

A.1 CREATION OF SITES

A.1.1 Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of St Mary's School.

A.1.2 Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

A.1.3 The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the Headteacher.

A.1.4 Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

A.1.5 The headteacher of relevant managers must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

A.1.6 There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school's brand and image.

A.1.7 Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

A.2 CHILDREN AND YOUNG PEOPLE

A.2.1 When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

A.2.2 When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying or prone to extremism and radicalisation.

A.2.3 If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

A.2.4 Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008)

A.2.5 Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

A.2.6 Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.

A.2.7 Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school or the County Council. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your Headteacher

A.3 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE

A.3.1 St Mary's School social media sites can be created only by or on behalf of the school. Site administrators and moderators must be St Mary's School employees or other authorised people.

A.3.2 Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the Headteacher.

A.3.3 Approval for participating, on behalf of St Mary's School, on sites created by third parties must be obtained from the Headteacher.

A.3.4 Content contributed to own or third-party hosted sites must be discussed with and approved by the Headteacher.

A.3.5 The school's Headteacher must be consulted about the purpose of the proposed site and its content and for the use of the school logo and brand.

A.3.6 Staff must complete the Social Media Site Creation Approval Form (Appendix B) and forward it to the school's Headteacher before site creation.

A.3.7 Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Headteacher immediately. Staff members must not communicate with the media without the advice or approval of the Headteacher.

A.4 CONTENT OF WEBSPACE

A.4.1 St Mary's School -hosted sites must have clearly expressed and publicised Terms of Use and House Rules. Third-party hosted sites used for work purposes must have Terms of Use and House Rules that conform to the school or County Council standards of professional conduct and service.

A.4.2 Staff members must not disclose information, make commitments or engage in activities on behalf of St Mary's School or the County Council without authorisation.

A.4.3 Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school's or County Council's image, reputation and services.

A.4.4 Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

A.4.5 Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

A.4.6 Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

A.4.7 St Mary's School -hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.

A.4.8 Staff members participating in St Mary's School -hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.

A.4.9 Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

A.4.10 Personal opinions should not be expressed on official sites.

A.4.11 Contributors must ensure that the school has permission from parent/carers for the use of any child's image on the site. The school office has class lists of any child who does not have this permission which contributors must refer to.

A.5 CONTRIBUTORS AND MODERATION OF CONTENT

A.5.1 Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.

A.5.2 Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.

A.5.3 The content and postings in St Mary's School -hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.

A.5.4 The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the Terms of Use and House Rules. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

A.5.5 For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.

A.5.6 Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.

A.5.7 Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the House Rules must not be posted or removed.

A.5.8 Any proposal to use social media to advertise for contributors to sites must be approved by the school's Headteacher.

A.5.9 Approval must also be obtained from the school's Headteacher to make an external organisation a 'friend' of the site.

APPENDIX B

St Mary's Catholic Primary School
Social Media Site Creation Approval Form

Use of social media on behalf of St Mary's School must be approved prior to setting up sites.

Please complete this form and forward it to the school's Headteacher.

TEAM DETAILS	
Department	
Name of author of site	
Author's line manager	

PURPOSE OF SETTING UP SOCIAL MEDIA SITE **(please describe why you want to set up this site and the content of the site)**	
What are the aims you propose to achieve by setting up this site? What is the proposed content of the site?	

PROPOSED AUDIENCE OF THE SITE
Please tick all that apply.

- ☐ Pupils of St Mary's School (ages 4 – 11)
- ☐ St Mary's School staff
- ☐ Pupils' family members
- ☐ Pupils from other schools (provide names of schools)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

PROPOSED CONTRIBUTORS TO THE SITE
Please tick all that apply.

- ☐ Pupils of St Mary's School (ages 4 – 11)
- ☐ St Mary's School staff
- ☐ Pupils' family members
- ☐ Pupils from other schools (provide names of schools)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

ADMINSTRATION OF THE SITE	
Names of administrators (the site must have at least 2 approved administrators)	
Names of moderators	

(the site must have at least 2 approved moderators)	
Who will vet external contributors?	
Who will host the site?	☐ St Mary's School ☐ Third party; please give host name
Proposed date of going live	
Proposed date for site closure	
How do you propose to advertise for external contributors?	
If contributors include children or adults with learning disabilities how do you propose to inform and obtain consent of parents or responsible adults?	
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' of the site?	

APPROVAL		
Headteacher **I approve the aims and content of the proposed site and the use of school brand and logo.**	Name	
	Signature	
	Date	

St Mary's Catholic Primary School

Loan Agreement for School Laptops and Removable Media

For the purpose of this agreement the term 'laptop' is used to describe any portable computer device including laptops, notebooks, tablets, cameras, flash drives, on which school data may be stored
Your school laptop is on loan to you while you remain employed by St Mary's Catholic Primary School. While the laptop is in your care the following points must be noted:

1. The laptop remains the property of St Mary's Catholic Primary School and is only for the use of the member of staff to whom it is issued. It must be returned to the school in an acceptable condition if and when that member of staff leaves the school's employment.
2. Only software licensed by the school, authorised by the ICT Co-ordinator/headteacher/ technician may be used.
3. Anti-virus software is installed and you are expected to check it is updating on a weekly basis.
4. Do not remove any programs installed on the laptop.
5. When using the laptop at school or away from school, the Acceptable Use Policy for Staff applies.
6. Any faults with laptops must be reported to the ICT Technician as soon as possible. Under no circumstances should staff attempt to repair suspected hardware or software faults. These are to be carried out only under the terms of the warranty.
7. Where remote access to the school network is available it is vital to log off when finished and to protect log-in details. This is to avoid unauthorised access to sensitive or shared material and to protect the school network from outside access by unauthorised users.
8. Any usage charges incurred by staff accessing the internet from home are not rechargeable to the school.
9. Within two weeks of the issue of a replacement laptop, the original laptop must be returned to the ICT Co-ordinator with 'My Documents' cleared and any additional programs added by the user removed. The original laptop may be re-issued to another adult or pupil user.
10. The laptop may be recalled for periodic maintenance, with appropriate notice given.

Device:	*e.g. laptop*		
Make:		Model:	
Serial number:		School asset register number (blue label):	
Device:	*e.g. laptop*		
Make:		Model:	
Serial number:		School asset register number (blue label):	
Device:	*e.g. laptop*		
Make:		Model:	
Serial number:		School asset register number (blue label):	

I confirm that I have received the removable media listed above and that I will comply with the Social Media and Acceptable Use Policy for Staff and Loan Agreement listed here.

Signed:	**Date:**
Name:	

~ Pray ~ Learn ~ Love ~ Enjoy ~