

St Hugh's Catholic Primary School

Use of Social Media Policy

1. Introduction

- 1.1 St Hugh's Catholic Primary School recognises its statutory responsibilities related to employment. Day to day management of staff is delegated to the Headteacher; ultimate responsibility lies with the Governing Body.
- 1.2 The Governing Body of St Hugh's Catholic Primary School is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites has become a very significant part of life for many people. They provide a positive way to keep in touch with family, friends and colleagues, and can be used to exchange ideas and thoughts on common interests. Examples of such sites include, but are not limited to, blogs (short for web logs), MySpace, Facebook, Bebo, YouTube, Windows Live Spaces, LinkedIn, forums, bulletin boards, multiplayer online gaming, chatrooms and instant messenger apps.
- 1.3 The Governing Body will ensure that all staff are made aware of this policy and any other related ICT protocols. This policy will be easily accessible to staff and the headteacher will make any new or temporary staff aware of this policy.
- 1.4 The Governing Body expect staff to keep a professional distance from students and to make a clear separation between their private social lives and those of students. Social networking between staff and students is prohibited. The exception to this is where the school social networking sites as a communication tool with parents, the community and the wider population (see 6.1.14)
- 1.5 It is important that all staff are able to use technologies and services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. The Governing Body must balance this with their duty to safeguard students and the reputation of the school and the wider community.

2. To whom does this policy apply?

This policy applies to all employees, governors and volunteers at the school.

3. Aims:

- to enable staff and volunteers to use social networking sites safely and securely
- to ensure staff and volunteers are aware of the risks associated with inappropriate use of social networking sites
- to safeguard staff and volunteers with respect to use of social networking sites and make sure they do not make themselves vulnerable
- to ensure the Governing Body maintains its duty to safeguard students and the reputation of the school
- to ensure duty of care towards staff and volunteers adversely affected

4. Legislation

This policy has taken account of the following legislation:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006

5. Responsibilities

The Governing Body will:

- a) ensure this policy is implemented
- b) ensure that all staff and volunteers have access to this policy and all new employees and volunteers are made aware of it
- c) seek professional advice and support from the Local Authority when necessary.

St Hugh's Catholic Primary School

Use of Social Media Policy

- d) take appropriate action, up to and including referring the matter to the police in the case of staff and volunteers being subjected to abuse on social media.

The headteacher will:

- a) know this policy and make sure that staff and volunteers also understand the policy and their own responsibilities
- b) ensure that staff and volunteers understand the risks of the use of social networking sites and the possible implications of inappropriate use
- c) instigate disciplinary procedures where appropriate
- d) seek advice from HR where necessary in the case of potential misuse

Staff will:

- a) behave responsibly and professionally in connection with their use of social networking sites
- b) co-operate with the headteacher and Governing Body in implementing this policy

6. Use of Social Networking Sites

For their own security, employees should regularly review their privacy settings on all their social networking sites; however all communication via social networking should be made with the awareness that anything said, shown or received could be made available intentionally or otherwise to an audience wider than that originally intended. If in doubt guidance should be sought from an appropriate manager.

- 6.1 Staff must not access social networking for personal use through school information systems or using school equipment
- 6.2 Staff must not accept students as friends - personal communication could be considered inappropriate and unprofessional, and makes staff vulnerable to allegations
- 6.3 In no circumstances should staff post photographs of students, except where the staff member's own children attend the school. In these circumstances, staff members may post images of their own children and friends at social events; members of staff should take care to ensure the suitability of the images and that they are not posted in relation to the school.
- 6.4 Staff are advised not to be friends with recent students; the potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking
- 6.5 Staff must not place inappropriate photographs on any social network
- 6.6 Staff must not post indecent remarks
- 6.7 If a member of staff receives messages via social networking that they think could be from a student, they must report it to their line manager and contact the internet service or social network so that they can investigate and take the appropriate action
- 6.8 Staff are advised not to disclose their affiliation with the school on their profile(s), or write about their work.
- 6.9 Staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual which could be in breach of the Data Protection Act.
- 6.10 Staff must not disclose any information about the school that is not yet in the public arena
- 6.11 Staff must not make defamatory remarks about the school / colleagues / students / parents or post anything that could potentially bring the school into disrepute.
- 6.12 Staff should not disclose confidential information relating to their employment at the school
- 6.13 Staff should avoid language which could be deemed as offensive
- 6.14 Where a school uses social networking for communication purposes, these networks can be accessed via school equipment. School will monitor this closely and only those with administrator rights should communicate in this way. Any misuse or abuse by staff, students or the wider community should be reported to the Headteacher

St Hugh's Catholic Primary School
Use of Social Media Policy

7. Breaches of the Policy

- 7.1 The Governing Body does not discourage staff from using social networking; however staff should be aware that they will take inappropriate use of social networking seriously. Any posts or comments which could be deemed online bullying or harassment will be dealt with in the same way as other instances of bullying or harassment.
- 7.2 The headteacher may take disciplinary action in the case of allegations of inappropriate use of social networking, depending on the seriousness of the allegations.
- 7.3 There may be instances where the school would be obliged to inform the police of any activity or behaviour where there are concerns about its legality
- 7.4 From time to time, staff and volunteers at school may be subject to abuse on social networking sites in connection with their role in school. Any such abuses should be reported immediately to the headteacher, who will inform governors and take whatever action is possible to deal with the situation and support the affected colleagues.

St Hugh's Catholic Primary School

Use of Social Media Policy

Policy: How will infringements be handled?

Whenever a student or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

STUDENT	
Category A infringements	Possible Sanctions:
Use of non-educational sites during lessons Unauthorised use of email, mobile phone (or other new technologies) in lessons e.g. to send texts to friends Use of unauthorised instant messaging / social networking sites	Refer to class teacher Escalate to: senior manager / Online-Safety Coordinator
Category B infringements	Possible Sanctions:
Continued use of non-educational sites during lessons after being warned Continued unauthorised use of email after being warned use of mobile phone (or other new technologies) after being warned Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups Use of File sharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc Trying to buy items online Accidentally corrupting or destroying others' data without notifying a member of staff of it Accidentally accessing offensive material and not logging off or notifying a member of staff of it	Refer to Class teacher / Online-Safety Coordinator Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent
Category C infringements	Possible Sanctions:
Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) Trying to access offensive or pornographic material (one-off) Purchasing or ordering of items online Transmission of commercial or advertising material	Refer to Class teacher / removal of Internet and/or Learning Platform access rights for a period Escalate to: contact with parents / removal of equipment Other safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site
Category D infringements	Possible Sanctions:
Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned Deliberately creating, accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 Bringing the school name into disrepute	Refer to Head Teacher / Contact with parents Other possible safeguarding actions: Secure and preserve any evidence Inform the sender's e-mail service provider. Liaise with relevant service providers/ instigators of the offending material to remove Report to Police / CEOP where child abuse or illegal activity is suspected
STAFF	
Category A infringements (Misconduct)	Possible Sanctions:
Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. Not implementing appropriate safeguarding procedures. Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community.	Referred to line manager / Head teacher Escalate to: Warning given

St Hugh's Catholic Primary School

Use of Social Media Policy

<p>Misuse of first level data security, e.g. wrongful use of passwords. Breaching copyright or license e.g. installing unlicensed software on network.</p>	
<p>Category B infringements (Gross Misconduct)</p>	<p>Possible Sanctions:</p>
<p>Serious misuse of, or deliberate damage to, any school computer hardware or software; Any deliberate attempt to breach data protection or computer security rules; Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; Bringing the school name into disrepute</p>	<p>Referred to Head teacher / Governors; Other safeguarding actions: Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. Identify the precise details of the material. Escalate to: report to LA /LSCB, HR Report to Police / CEOP where child abuse or illegal activity is suspected. ,</p>
<p>If a member of staff commits an exceptionally serious act of gross misconduct The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.</p> <p>Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Schools HR team</p>	
<p>Child abuse images found</p> <p>In the case of Child abuse images being found, the member of staff should be immediately suspended and the Police should be called.</p> <p>Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):</p> <p>http://www.ceop.gov.uk/reporting_abuse.html</p> <p>http://www.iwf.org.uk</p>	
<p>How will staff and students be informed of these procedures?</p> <ul style="list-style-type: none"> • They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement form; • Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online-safety / acceptable use agreement form; • The school's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school. • Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents. • Staff are issued with the 'What to do if?' guide on online-safety issues. 	

St Hugh's Catholic Primary School

Use of Social Media Policy

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

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- 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, or a responsible adult has approved.
- 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 only ever previously 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.

I have read and understand these rules and agree to them.

Signed: _____ Date: _____

Class _____

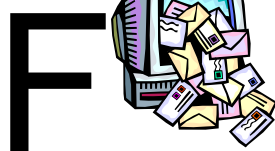
Think before you click



I will only use the Internet
and email with an adult



I will only click on icons and
links when I know they are
safe



I will only send friendly and
polite messages



If I see something I don't
like on a screen, I will
always tell an adult

My Name:

My Signature:

St Hugh's Catholic Primary School
Use of Social Media Policy

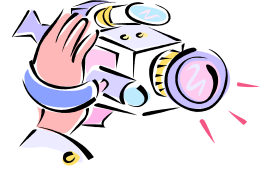
<p>Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter / son access to:</p> <ul style="list-style-type: none"> ○ the Internet at school ○ the school's chosen email system ○ the school's online managed learning environment ○ ICT facilities and equipment at the school. 		
<p>I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.</p>		
<p>I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.</p>		
<p>Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.</p>		
<p>I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.</p>		
<p>I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.</p>		
<p>I will not take and then share online, photographs of other children (or staff) at school events without permission.</p>		
<p>Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this</p>		
<p>I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.</p>		
<p>I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.</p>		
<p>My child's name:</p>	<hr style="border: none; border-top: 1px solid black;"/>	
<p>Parent / guardian signature:</p>	<hr style="border: none; border-top: 1px solid black;"/>	
<p>Date</p>	<hr style="border: none; border-top: 1px solid black;"/>	

St Hugh's Catholic Primary School
Use of Social Media Policy
The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

- **If the pupil is named, we avoid using their photograph.**
- **If their photograph is used, we avoid naming the pupil.**



Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
e.g. taking photos or a video of progress made by a Reception child, as part of the learning record, and then sharing with their parent / guardian.
- Your child's image being used for presentation purposes around the school;
e.g. in class or wider school wall displays or PowerPoint® presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

St Hugh's Catholic Primary School

Use of Social Media Policy

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**



How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- **We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.**

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:

<https://www.thinkuknow.co.uk/parents/browser-safety/>