OCKLYNGE JUNIOR SCHOOL

SUITE OF I.T. SAFETY POLICIES

Date approved by Governors	June 2018
Date of Next Review	June 2019
Status	MAT Statutory

CONTENTS:

Ocklynge Junior School Online Safety Policy

This policy should be read in conjunction with the schools Computing Policy, Social Media Policy, Staff AUP and 'Internet Golden Rules'.

Background

As with any system as large as the internet there are risks, but the advantages of working in a connected world, far outweigh them. At Ocklynge we take e-safety seriously and review our practices and procedures annually.

Communication

All communication that takes place between staff and outside agencies must take place through the school sanctioned media e.g. school website, Class Dojo, or in rare cases, the school Facebook.

Internet safety

It is acknowledged that there are inappropriate and offensive materials on the internet. There are also people who seek to abuse the internet. To avoid pupils accessing such sites, they will not be given access to the Internet without adult supervision. The school's internet is filtered by Schools following the advice from County. In the event of inappropriate material not being screened out, the school will take proactive measures to inform parents and Schools ICT so that the website concerned is blocked. The school monitors all internet activities accessed by pupils and staff.

Children are taught online safety through the Rising Stars Computing scheme of work during Computing lessons with additional content in PSHEe lessons, following the SWGFL We expect children to exercise a growing awareness and use of safe practices.

If there is an incident of deliberate inappropriate use of school equipment, the evidence trail will be preserved. Two people will bag up the workstation and sign for it. The DSL (Sylvia Berhane) is then responsible for taking appropriate action.

Internet Use Guidelines

To ensure that pupils benefit from the school's Internet resources, all pupils are expected to adhere to the guidelines in 'The Internet Golden Rules' document.

Pupil's Acceptable Use Policy

During the first week of the new academic year the pupils are required to understand and sign the class Internet Golden Rules.

Procedures for dealing with breaches of the Acceptable Use Policy

If a pupil is found to have been trying to access unsuitable sites, sending threatening or offensive e-mails, or breaking any other of the Acceptable Use Policy guidelines, appropriate action will be taken. The incident will also be dealt with in accordance with

the school discipline policy. The same procedures will apply to message posted on blogs or forums. Cyber bullying, (using the internet to intimidate, threaten or bully others) is totally unacceptable. The school makes no distinction between where or when such events occur. If it happens, we want to know about it and will deal with it accordingly. Parents or pupils who encounter online issues, are encouraged to use the normal channels of communication to bring these to the attention of the school.

If any member of staff encounters a breach of the Online Safety policy, they must fill in an incident form, isolate any machines involved, and inform Sylvia Berhane or Andy Gietzen

School Intranet

Staff have a unique, strong password that is needed to access the School's Network. These passwords are changed regularly. Pupils also have a username that allows them access to the Public Drive, and their own drive.

Staff AUP

Staff are provided with access to the Internet at school, but must first sign the Acceptable Use Statement for Staff.

School Web Site

Children will only be identified by first names. Photographs of children will not be accompanied by names. Parents are informed of this via the school Information handbook, and they may contact the school if they would rather their child's photograph was not used.

Class Dojo

Class Dojo will be used by staff to enable one-to-one messaging to take place between teachers and parents. Teachers are also able to post group messages and photos to all the connected parents in their class. The groups are 'invite only' and parents are provided with a code to enable access, the class teacher then allows the parent to join the group. It is expected that class teachers will follow all other rules for posting images on the internet within this policy.

Acceptable Computer/Internet Use Statement for Staff - September 2018-19

The computer system and the school laptops are owned by the school and are made available to staff to enhance their professional activities, including teaching, research, administration and management. This policy has been drawn up to protect all parties – the pupils, the staff and the school and applies to the use of computers inside and outside of school.

All staff with access to the school system should read, sign and return this policy to the Computing Subject Lead.

- I understand that the School will monitor my use of the school digital technology and communications systems.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use when this does not impact on the pupils learning.
- I will not disclose my password to others or record it in a place that can be accessed by others. My password will include a capital letter, a number or symbol and be at least 8 characters long.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's Social Media Policy.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Schools policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage, where possible.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Members/Trustees/Governors and/or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

- Staff / Volunteer Name: .....
- Signed: .....
- Date: .....

Photography and Video Policy 2018-19

Principles

This policy details the rules governing photography and recording videos at the school, the distribution of these photos and videos, and their publication on the internet. It covers the rules for staff, governors and parents, and is founded on four main principles:

Safety

The overriding priority is to ensure that photography does not lead, either directly or indirectly, to anything that may potentially endanger the safety of the children at the school.

Privacy

We believe that every child and parent is entitled to their own privacy, and can therefore choose not to feature in photographs or videos recorded at the school.

Projecting the right image

Photographs taken at school should not do anything that may cause embarrassment to the school, the children, or the staff.

Sharing children's achievements

It is natural for every parent to want to share their children's activities and achievements at school with their friends and family. This school is keen to allow this as much as possible, while keeping this in balance with the first three principles.

Consent

When a child joins the school, their parent or guardian is asked for consent for the child to appear in photos on the school website. The school encourages all parents to provide consent, as it enables us to include all the children in depictions of school life, but we recognise and respect the right to refuse consent.

Parents may withdraw consent at any time, or grant consent if they had previously declined.

School Website

The school endeavours to publish on the school website and social media a selection of photos and videos of school events and general school life. Any material published to the website must be assessed to ensure it meets the following safeguarding rules:

1. It must not feature any child whose parent or guardian has not given consent.

2. It must not offer any means of identifying a child by name.

3. It must not in any way embarrass the school or the children and staff involved.

4. It should usually not include any child who left the school more than one year ago.

Rule 4 is worth explaining in more detail. Most children are excited to see photos or videos of themselves on the school website. But as they get older, they are not always so enthusiastic about reminding themselves, or

others, of their younger selves. The school will therefore endeavour to remove older photos featuring children who have left the school some time ago in order to avoid any embarrassment or discomfort it may cause them.

Photos and video intended for the school website should be taken either by a member of staff, or another person (typically a governor or parent) authorised by the **Headteacher**. These photos and videos must be approved by the **Headteacher** prior to publication on the website; the mechanism for doing this should be agreed by the **Headteacher** and the photographer.

Rules for Parents, Guardians and Governors

Parents and guardians are permitted to take photographs and record videos at designated school events, as long as they agree to the conditions described in this policy.

These events include:

- Musical Events;
- Sports Day;
- Nativity Plays;
- Class Assemblies;
- Friends of Ocklynge events held in school.

At these events, photos may only be taken at the location of the event. Parents, Guardians and Governors are not permitted to take photos in classrooms or elsewhere in the school unless explicitly authorised by the **head teacher.**

Outside designated events

It is not permitted to use a camera on school premises at any time outside these designated events unless explicitly authorised by the **Head teacher**.

Distribution and publication of photos and videos

Photos taken at these events are for your own personal use only. They may be shared by email with friends and family, but must not be published on any internet site. This includes Facebook, Twitter, YouTube, Pinterest and all other social media services.

The reason for this restriction is that it is not possible for individual parents to ensure that all four of the safeguarding rules described above are adhered to at both the time of publication, and later.

Withdrawal of permission

Failure to adhere to these conditions may, at the discretion of the Headteacher, lead to a withdrawal of permission to use a camera at future events.

Rules for Staff

Staff may take photos and video anywhere within the school for the purposes indicated on the parental consent form.

These may be published on the school website if they conform to the safeguarding rules described above.

They may not be published on any other internet or social media site.

Subject to approval of the **Headteacher**, photos and videos may be stored on secure, password-protected internet services for archival or transfer purposes.

They may be stored on password-protected staff laptops. They should be deleted once they are no longer needed, or when the featured children have left the school.

They may be shared with other members of staff by email to support teaching work. They may not be shared with friends and family.

The school cameras should always be used to take photographs.

Staff must not use their mobile phone to take photos or videos of any pupils or school events.

Members of staff who are also parents or guardians of children at the school are permitted to take photographs at school events under the terms described in “rules for parents, guardians and governors”.

External Photographers

Terms for external photographers, such as local newspaper photographers, must be agreed in advance with the **Headteacher**. These are considered on a case-by-case basis, and must conform to the safeguarding rules described above.

Social Media

1 INTRODUCTION

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 maintaining pages on internet encyclopaedias such as *Wikipedia*.

While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Ocklynge Junior School staff, governors, volunteers and contractors are expected to follow when using social media.

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 and East Sussex County Council are safeguarded.

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

2 SCOPE

This policy applies to Ocklynge Junior School's 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.

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 (see sections 5, 6, 7 and Appendices A and B).

This policy applies to personal webspace such as social networking sites (for example *Facebook*, *MySpace*), blogs, mircoblogs 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

Ocklynge Junior 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, and
- the Data Protection Act 1998.

Confidential information includes, but is not limited to:
Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
Information divulged in the expectation of confidentiality
School 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 Ocklynge Junior School 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 Ocklynge Junior School liable to the injured party.

4 RELATED POLICIES

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

- Code of Conduct for Employees
- Ocklynge Junior School online safety policy.

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 and your personal interests.

5.2 You must not engage in activities involving social media which might bring Ocklynge Junior school into disrepute.

5.3 You must not represent your personal views as those of Ocklynge Junior School or on any social medium.

5.4 You must not discuss personal information about pupils, Ocklynge Junior School 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, and abuse or defame pupils, their family members, colleagues, other professionals, and other organisations, Ocklynge Junior School.

5.6 You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Ocklynge Junior School.

6 PERSONAL USE OF SOCIAL MEDIA

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

6.2.0 Staff members should not contact with pupils on social media and there must be a valid personal reason for doing so, for example community based club or society.

6.2.1 Ocklynge Junior 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.

6.2.2 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.

6.2.3 If staff members wish to communicate with pupils for a curriculum activity through external websites 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 or website to which the school has a subscription.

6.2.4 Subject to Staff 6.2 staff members must decline 'friend requests' from pupils they receive through their personal social media accounts. If a pupil makes a friend request then you are to inform the safeguarding lead who will then contact the pupils' parents.

6.2.5 On leaving Ocklynge Junior School's service, staff members must not contact Ocklynge 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, and other parties and school corporate, information must not be discussed on their personal webspace.

6.9 Any school business related photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school uniforms or clothing with school logos or images identifying sensitive school must not be published on personal webspace.

6.10 School 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 Ocklynge Junior School, service or team logos or brands must not be used or published on personal webspace.

6.13.1 Ocklynge Junior School does not permit the use of social media for personal reasons whilst at work.

6.13.2 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.

6.13.3 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 Ocklynge Junior School

7.1 Staff members can only use official school sites for communicating with pupils or to enable pupils 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.

8 MONITORING OF INTERNET USE

8.1 Ocklynge Junior School monitors usage of its internet and email services without prior notification or authorisation from users.

8.2 Users of Ocklynge Junior 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.

9 BREACHES OF THE POLICY

9.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Ocklynge Junior School Disciplinary Policy and Procedure.

9.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Ocklynge Junior School or any illegal acts or acts that render Ocklynge Junior School liable to third parties may result in disciplinary action or dismissal.

9.2.1 Contracted providers of Ocklynge Junior School services must inform the relevant school 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. Any action against breaches should be according to contractors' internal disciplinary procedures.

APPENDIX A

Requirements for creating social media sites on behalf of Ocklynge Junior 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 Ocklynge Junior 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 initially with the ICT coordinator and 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, on-going time commitment.

A.1.5 The headteacher or 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. It must be remembered that any page created is likely to be accessible indefinitely, even if the original is removed.

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.

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, the safeguarding lead or the Head Teacher 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 and the 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. 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 online safety team (or appropriate manager).

A.3 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE

A.3.1 Ocklynge Junior School social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Ocklynge Junior 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 online safety team.

A.3.3 Approval for participating, on behalf of Ocklynge Junior School , on sites created by third parties must be obtained from the online safety team.

A.3.4 Content contributed to own or third-party hosted sites must be discussed with and approved by the staff member's line manager.

A.3.5 The school's Headteacher must be consulted about the purpose of the proposed site and its content. In addition, the Headteacher's approval must be obtained 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 online safety team before site creation. 18

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

A.4 CONTENT OF WEBSPACE

A.4.1 Ocklynge Junior 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 standards of professional conduct and service.

A.4.2 Staff members must not disclose information, make commitments or engage in activities on behalf of Ocklynge Junior School 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 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 Ocklynge Junior 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 Ocklynge Junior 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.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 Ocklynge Junior 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 an approved administrator 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, inciting extremist views or hatred or those likely to put a young person or adult at risk of harm , for example child sexual exploitation, 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 online safety team to allow an external organisation a 'friend' of the site.

APPENDIX B

Ocklynge Junior School

Social Media Site Creation Approval Form

Use of social media on behalf of Ocklynge Junior School must be approved prior to setting up sites.

Please complete this form and forward it to the school's **online safety team**

Department	
Name of author of site	
Author's line manager	

What are the aims you propose to achieve by setting up this site? What is the proposed content of the site?

- ☐ Pupils of Ocklynge Junior School
- ☐ Ocklynge Junior School staff
- ☐ Pupils' family members
- ☐ Pupils from other schools (provide names of schools)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

- ☐ Pupils of Ocklynge Junior School
- ☐ Ocklynge Junior School staff
- ☐ Pupils' family members
- ☐ Pupils from other schools (provide names of schools)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

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?	☐ Ocklynge Junior 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?	

Line Manager **I approve the aims and content of the proposed site.**	Name	
	Signature	
	Date	
ICT coordinator **I approve the aims and content of the proposed site and the use of school brand and logo.**	Name	
	Signature	
	Date	
Headteacher	Name	
	Signature	
	Date	