# DERBYSHIRE LA

# Acceptable Use of IT, the Internet and Electronic Communication Policy

# FLAGG NURSERY SCHOOL

**Record of Policy Amendment / History**

| Version/ Issue | Date | Author | Reason for Change |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# CONTENTS


1. Introduction
2. Scope
3. Use of Internet, Email and other Electronic Communication
4. Safe Working Practice
5. Virtual Learning Environment
6. Social Media
7. Safeguarding
8. Newly Qualified Staff
9. Laptops issued to Staff
10. Health and Safety guidance on using IT equipment including Laptops
11. Use of other School IT Equipment
12. Software
13. Network Access, Passwords and Data Security
14. Encryption
15. Monitoring of Email
16. Monitoring Internet Access and Instant Messages
17. Private Use
18. Disciplinary and Related Action
19. Summary

Acceptable Use Agreement

Appendix 1 - Employee Guidance on use of Social Media

Appendix 2 - Additional Guidance for Headteachers on the use of Social Media

1. **Introduction**

The School's IT resources are essential to the effective delivery of educational provision. Computers and other networked facilities, including internet access, are available to staff and pupils within the school and should be used to promote educational learning. It is therefore vital that all staff, agents and contractors are aware of the School's policies and procedures relating to the use of IT resources. A poorly administered network or weak password controls could expose the School's information to an unauthorised user or introduce a virus infection.

**2. Scope**

2.1 This policy applies to all technology and communications equipment provided by Derbyshire County Council/School (e.g PCs, laptops, PDAs, Palm computers, mobile phones with Internet access etc).

2.2 Any personal or potentially personal information sent via e-mail and the Internet is covered by the Data Protection Act 1998. The Act requires all employees to take special care when handling personal information.

2.3 E-mails may be covered by the Freedom of Information Act and are disclosable as part of legal proceedings. Employees should exercise the same caution when writing e-mails as they would in more formal correspondence.

2.4 Use of e-mail and the Internet, which brings the County Council/school into disrepute, may result in disciplinary action.

2.5 Limited use of the Internet and e-mail is permitted subject to these principles:

a. E-mail: Employees are allowed limited use of e-mail for personal communication
b. Internet: Personal use of the Internet is permitted outside normal working hours
c. Any personal use must not, in any way, distract employees from the effective performance of their duties

**3. Use of Internet, E-Mail and other Electronic Communication**

Internet and Email use is integral to the effective delivery of educational services provided by the school. Nothing in this policy should be read as restricting the proper use of email and Internet for School activities. Limited personal use of School's Internet and Email system is permitted subject to these principles and guidance notes.

Email

3.1 Where possible, personal use of email should be in employees' own time. Limited use of email during the working day is allowed, but should be restricted to a few minutes a day to respond to urgent incoming email and should not be used when teaching or supervising pupils.
Excessive use of email is not allowed and may result in disciplinary action.

3.2 While personal use of the Internet and email is permitted during lunch breaks and out of working hours, staff should be aware that the facilities are provided by the school and any activity received/sent through the school's network, personal or otherwise, is recorded and will be monitored.

3.3 Staff should not engage in 'recreational' chatting during working time, on email or through instant messaging, that results in lost productivity or distracts other employees from their work. The school's facilities must never be used for the passing of inappropriate personal information of any kind.

3.4 Email is now used widely to communicate both internally and externally, providing rapid circulation and many positive benefits. Staff should, however, remain aware of their professional position when communicating via email. When email is used to communicate with students, parents or carers as part of a professional role, a school email address should always be used. The style and format of any such communication should follow guidelines provided by the school. Staff should consider whether it is advisable to copy a colleague into any contact with a pupil or parent as a further safeguard.

Staff should be aware that email is not always the best form of communication and should consider alternatives, as appropriate.

3.5 Improper statements in email can give rise to personal liability and liability for the school and may constitute a serious disciplinary matter. Emails that embarrass, misrepresent or convey an unjust, or unfavourable, impression of the school or its business affairs, employees, suppliers and their families are not permitted.

3.6 Extreme care must be taken when using the school's email facilities to transmit information. Confidential or sensitive information should not be sent via the Internet or email unless the data is protected by the school's secure provision for such communications. Staff should remember that when a Subject Access Request or Freedom of Information request is submitted relevant email communications will be included in the material to be provided.

3.7 Employees must not use e-mail in any way that is insulting or offensive.

Employees must not deliberately view, copy or circulate any material that:

- could constitute bullying
- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcome propositions
- contains images, cartoons or jokes that will cause offence

- appears to be a chain letter

3.8 Personal use of Internet

- Use of the Internet is limited to employees' own time.
- Use of the Internet via County Council or school equipment should exclude use for trading or personal business purposes.
- Use of the Internet to buy goods or services will not render the County Council or school liable for default of payment or for the security of any personal information disclosed. Staff are advised not to use the school's computer system for making payments.
- Personal goods must **not** be delivered to the School.

3.9 Site Contents

Many Internet sites contain unacceptable contents. Employees must not deliberately view, copy or circulate any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material, the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains images, cartoons or jokes that will cause offence
- that constitutes bullying

3.10 Accidental Access to Inappropriate Material

Many internet sites that contain unacceptable content are blocked automatically by the school's filtering systems. However it is not possible to block all 'unacceptable' sites electronically in all circumstances. If staff become aware of any sites that require re-categorisation they should inform the school's IT technician as soon as possible. Employees may receive an e-mail or visit an Internet site that contains unacceptable material. If this occurs, a line manager or the headteacher should be informed as soon as possible. The headteacher will use their professional judgement whether to report the matter further. In this situation the staff member should ensure a short written record is kept as they may be asked to provide details relating to the incident and an explanation of how it occurred. This information may be required later for management or audit purposes.

3.11 Copyright

Employees may be in violation of copyright law if text is simply cut and pasted into another document. This may equally apply to photographs and music samples used as illustration or backing track in resource materials. Teachers should make it clear to pupils that care should be taken when including this type of material in any school or exam work. Most sites contain a copyright notice detailing how material may be used. If in any doubt about downloading and using material for official purposes, legal

advice should be obtained. Unless otherwise stated on the site all down loaded material must be for curricular or research purposes and must not be passed to third parties.

Downloading of video, music files, games, software files and other computer programs – for non-work related purposes-is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.

## 4. Safe Working Practice

4.1 Staff should make careful, considerate use of the school's IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.

4.2 Staff are responsible for maintaining the security of computers and networks by only using their own logon details and not allowing other staff or pupils to use their personal passwords. Staff should ensure that machines are not left unattended when they are logged on.

4.3 Staff should ensure as far as possible, that when using work equipment at home, other family members do not use the equipment for their personal use. Staff are responsible for all the content (software and data) on any equipment allocated to them.

Staff should not install any unlicensed software on machines allocated to them.

4.4 Staff must make every endeavour to protect students from harmful or inappropriate material accessible via the Internet or transportable on computer media, in compliance with the school's system.

## 5. Virtual Learning Environments (VLE)

5.1 As many schools now provide 24 hour access to a wide range of information – including resource materials, pupil data, school policies – it is essential that clear guidelines are in place for the use of the VLE or portal, by both staff and pupils.

Network managers have a duty to ensure that the site access is secure with passwords providing differing levels of access to staff and students.

5.2 There must be no expectation by the school that staff will be available outside normal working hours just because they are able to access the VLE from home. There will therefore be no expectation, other than by agreement, that staff will respond to email or other messages, sent outside the working day, before the start of the next working day. It will be made clear to parents that if pupils are posting work on the site, or emailing work directly to a member of staff, that there must be no expectation of an immediate response.

5.3 Access to a VLE from outside school should not be a reason to reduce timescales for completion of work by either staff or pupils. For example, the same amount of time should be allowed for completion of annual reports if done on-line through the VLE as that allocated previously for hand-written reports.

## 6. Social Media

6.1 For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as Twitter, Facebook, LinkedIn, internet newsgroups, and chat rooms. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr.

There are many more examples of social media than can be listed here and this is a constantly changing area. These guidelines should be followed in relation to any social media used.

The use of sites such as Facebook, MSN, Messenger, Twitter, Skype and many others (such as on-line gaming through Xbox or PlayStation live) is now increasingly widespread. However, as well as bringing many positive benefits, there are also many potential problems. The following guidance is given to all staff and pupils for their own protection. The guidance should apply whether the staff member is using school hardware or their own personal hardware (computer, phone, console etc.)

6.2 At all times, staff should be aware of the School's Code of Conduct expected of professional adults working with children. Employees who work directly with members of the public, including parents, need to be aware that the information they post on their profile can make them identifiable to members of the wider school community as well as people they know in a private capacity.

Employees should therefore consider this when setting up their profile, particularly in relation to; the use of a photograph, providing details of their occupation, employer and work location.

Staff should consider very carefully any conflict of interest when linking through social media to people they also know through work. The School considers it would be inappropriate to have pupils as 'friends' through social media, and consequently, to do so may be considered to be a disciplinary matter.

Online sites such as Facebook are in the public domain, and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Also if a user's profile is linked to other sites, any changes to their profile will be updated there too. Staff who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard and therefore comments, photographs or video clips sent to such contacts may be more widely available than originally anticipated.

Staff should be aware of the image they are presenting when communicating via such media and ensure, as far as possible, that any comments made are not open to misinterpretation. Circulation of comments on such media can be rapid and widespread and therefore staff should be encouraged to adopt the general premise of not putting anything on such a site (or in an email) that they would not put in a formal letter, be prepared to say in a face-to-face conversation or discuss in a public place.

6.3 The Headteacher and Governors will give consideration, when reaching decisions relating to potential disciplinary cases for breach of such a code, to the difficulty of staff members in 'controlling their image' all the time, and that manipulation by others is extremely easy. The Head/Governors will give consideration to whether the 'image' had been created voluntarily by the member of staff.

6.4 All employees are expected to behave appropriately and responsibly, and should be aware that they may be accountable to the School for actions outside of their work.

This policy clarifies that online conduct is the employee's responsibility, and it is important that staff are aware that posting information on social networking sites cannot be isolated from their working life.

Any information published online can be accessed around the world within seconds and will be publicly available for all to see, and is not easy to delete/withdraw once published. The School views any comment that is made on a social media site as made publicly, and that any inappropriate comment made, will be considered in the context of which it is made. Staff are advised to be mindful that nothing on a social media site is 'private' so comments made must still meet the standards of the Employee Code of Conduct and other relevant policies.

Staff may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of School's policies, impacts on or compromises the employee's ability to undertake their role, or undermines management decisions. Such behaviour would be investigated and may result in disciplinary action being taken, and ultimately could result in dismissal.

6.5 Many staff will use social networking outside of work to keep in touch with family, friends or activity groups. For some staff in particular, there may be occasions when contacts within these situations result in links between staff and pupils at the school (for example where there is a pre-existing friendship with the parent of a pupil). Staff should ensure that in such circumstances they are able to make a professional distinction between their role as a 'friend' outside work and their role within work and clarify their position to such contacts.

6.6 Whilst generic political discussion is not to be discouraged, any communications that employees make through social media must not:

- bring the school into disrepute, for example by:

- criticising, disagreeing or arguing with parents, colleagues or managers
- making defamatory comments about individuals or other organisations/groups;
- posting images that are inappropriate or links to inappropriate content;

- breach confidentiality, for example by:
- referring to confidential information about an individual (such as a colleague or pupil) or the School

- do anything that could be considered discriminatory against, or bullying or harassment of, any individual or group of individuals, and in contravention of the School's policies, for example by:
- making offensive or derogatory comments relating to sex, gender
- reassignment, race (including nationality), disability, sexual orientation,
  religion or belief or age;
- using social media to bully another individual (such as an employee of
- the organisation); or
- posting images that are discriminatory or offensive or links to such content.

- take other action that impacts on the employee's ability to do their job, for example by:
- online activity that is incompatible with the position they hold in the School
- any breach occurring inside or outside the workplace that is likely to affect the employee doing his/her work.

- contravene the School's policies, for example;
- the Employee Code of Conduct, the Harassment and Bullying policy, or the Equalities policy.

The above examples are not a definitive list of the misuse of social media, but are examples to illustrate what misuse may look like.

6.7 Staff should use common sense when posting items, think about the intended audience and consequences of making unwise remarks about colleagues at the school.

6.8 Staff should be aware of the potential risks of communicating with current and ex-pupils in ways which may be considered as inappropriate – particularly if it could be shown that the adult-pupil relationship of trust had been breached. The School requires staff to only use school platforms to communicate with pupils, in line with the Safeguarding Policy.

Staff should report any inappropriate contact from pupils to a member of SLT at the earliest opportunity to prevent situations from escalating.

Staff are reminded that, as a safeguarding issue, they should always be careful about who they are 'talking to'. It is very easy to hide an identity in an on-line conversation.

6.9 Staff are reminded that they have a responsibility to report any racist, sexist or other discriminatory comments they become aware of through postings or chat on such sites.

Staff not allowed to access social media websites from the school's computers or devices during working time and they must not be left running "in the background", whilst at work. These provisions also apply to personal computers and mobile devices.

Leaving social media sites 'running' constantly in work's time is considered to be a breach of the acceptable use of the internet policy, and would be considered to be using School resources for personal use, in work's time, and such would be investigated under the Disciplinary procedure.

(See Appendix 1 for further guidance for Headteachers and Staff members)

## 7. Safeguarding

7.1 With the increased access of both pupils and staff to electronic communication, there is an increased chance of a disclosure being made to a member of staff through such a medium. It is increasingly likely that such a disclosure will be made outside normal working hours. Clearly, if the member of staff is not 'logged on' (and there is no expectation that they will be), then they cannot be faulted for taking no action until they receive the message during the next working day. The member of staff will then be expected to follow the normal school procedures for reporting a disclosure.

*(A further useful reference source is the Government Offices booklet "Guidance on Safer Working Practice for Adults Who Work With Children and Young People")*

## 8. Newly Qualified Staff

8.1 There can be particular issues for newly qualified staff relating to the use of social network sites. It is likely that throughout their training period, they will have been regular users of such sites and have possibly been less concerned about the content of their 'pages' or the image they have presented of themselves. As part of their induction, they should be made aware of the issues raised above as a matter of urgency and be advised to remove any material from such sites that may harm their new professional status. As many newly qualified staff may be not much older than some of the pupils they will be working with, it is extremely important that they are made aware at a very early stage of the potential problems (including loss of job) that inappropriate comments and contact on social network sites (even if outside working hours) can cause.

## 9. Laptops issued to staff

9.1 The laptop remains the property of the School and is provided to users on a loaned basis. The laptop provided must not be used by any person(s) other than the authorised user to whom it has been allocated and the property identification tag attached to each laptop should not be removed for any reason.

9.2 School laptops have a predetermined list of software installed on the hard drive. No addition or deletion of any software or hardware is permitted without the express permission of the Head Teacher or School IT Technician. To ensure that security patches and virus definitions are up to date staff should connect the laptop to the School network on a regular basis.

9.3 All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, the laptop should never be left in a vehicle overnight or other unsecured, vulnerable situation. Any loss or damage to School IT equipment should be immediately reported to the Head Teacher or School IT Technician.

9.4 When a contract of employment at the School ends, the employee must return all computer equipment and software to the School IT Technician in full working condition. The user account and all personal work stored on the laptop will then be securely deleted.

9.5 If software/hardware problems arise, the laptop may need to be restored to its original settings. Work files may be lost during the restoration process, therefore it is the responsibility of all users to ensure that backups of all files are regularly made to an external device, such as the School's networked server or encrypted mobile device.

9.6 Where there is evidence that the laptop has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any School laptop whilst on loan.

## 10. Health and Safety guidance on using IT equipment including laptops

10.1 In the interests of health and safety, staff are advised to adhere to the following recommendations for the safe use of personal laptops. Any health and safety concerns associated with the use of laptops should be discussed with the Head Teacher.

- Sit in a chair that provides good back support to avoid backache and position the laptop directly in front of the user to avoid twisting;
- Take regular breaks from the screen to reduce eyestrain.
- Avoid using the laptop on a low table or on the lap as both of these positions will increase strain on the neck and lower back.

This is not an exhaustive list of advice pertaining to health and safety issues. The HSE publication 'Work with Display Screen Equipment:

Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health & Safety (Miscellaneous Amendments) Regulations 2002 provides further information and guidance.

## 11. Use of other School IT Equipment

11.1 Users who borrow equipment from the School must sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use. Any loss or damage to equipment on loan should be immediately reported to the Head Teacher or School IT Technician in the first instance and any theft or criminal damage should be reported to the Police.

11.2 To prevent data loss and ensure consistent application of School policies no personally owned equipment should be attached to the School's network without the permission of the Head Teacher. All mobile devices must be encrypted or password protected wherever technology allows.

## 12. Software

12.1 Users should use software in accordance with applicable licence agreements. To copy software or any supporting documentation protected by copyright is a criminal offence. The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the School. Under no circumstances should any user possess unlicensed software on School premises or use unlicensed software on School IT equipment (including portable equipment).

## 13 Network Access, Passwords and Data Security

13.1 Users must only access information held on the School's computer systems if properly authorized to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the School network or IT equipment be disclosed to unauthorised persons. If you accidentally access information, which you are not entitled to view, report this immediately to the Head Teacher or School IT Technician.

13.2 Staff using computers in classrooms must ensure that sensitive data is not accessible to students or other individuals by logging off or locking the computer. In other areas computers must not be left logged on when unattended.

13.3 Staff passwords must be at least eight characters in length, containing at least one capital letter and one number. Whilst the user account is active the password must be changed on a regular basis, at least termly. System and administration level passwords should also be changed, at least on a termly basis.

13.4 All passwords are to be treated as sensitive, confidential information. Therefore, staff must not:

- write down passwords or store them on-line.
- use School user account passwords for other types of access (e.g., personal ISP accounts, Internet banking, etc.).
- share passwords with anyone, including line managers, colleagues, administrative assistants, secretaries, or IT Technicians.
- reveal a password over the phone or in an e-mail message or other correspondence.
- talk about a password in front of others including family members.
- hint at the format of a password (e.g., "my family name").
- reveal a password on questionnaires or security forms.
- insert passwords into e-mail messages or other forms of electronic communication.

13.5 If an account or password is suspected to have been compromised, the incident must be reported immediately to the Head Teacher or School IT Technician so that the account password can be changed.

## 14. Encryption

14.1 Sensitive or confidential information held on laptops or other portable devices (e.g. memory sticks) should be minimised. Staff should clarify with the headteacher the nature of material that may be held on these devices, for how long and with what security measures. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done with extreme care, following the school's security protocol, using an encrypted memory stick provided by the School, where required.

## 15. Monitoring of email

15.1 The school reserves the right to make appropriate arrangements to monitor, log record and access all communications at any time without notice. Initially this is done via an electronic system, however if this was triggered by an employee's actions, this would be reported to the Headteacher. Where there was good cause, this situation would be more closely monitored by the school's Network Manager, but only if explicitly requested in writing by the Headteacher. The Headteacher will record the reason for the monitoring. Whenever an employee's emails have been accessed/monitored, they will be notified and given the reasons in writing. Other than this employees should be assured that no-one is allowed to read/access their emails.

The following details are recorded by the system in respect of every email message:

- name of the person sending the email,
- the email addresses of all recipients and copy recipients,
- the size and name of any file attachments,
- the date and time sent,
- a copy of the email,
- a copy of file attachments.

15.3 The school may produce monitoring information, which summarises email usage and may lead to further enquiries being undertaken.

Monitoring information will be kept for six months.

## 16. Monitoring Internet Access and Instant Messages

16.1 Derbyshire County Council records the details of all Internet traffic. This is to protect the Council and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

The logs record:

- the network identifier (username) of the user,
- address of the Internet site being accessed,
- where access was attempted and blocked by the system,
- the Web page visited and its content,
- the name of any file accessed and/or downloaded,
- the identity of the computer on the network and the date and time.

Data contained in these logs will be monitored regularly by Audit Services to identify inappropriate use and the reports produced from the system will be sent to Chief Officers and Corporate IT as required to fulfil their responsibilities. Any excessive or inappropriate use could result in the facility being withdrawn or disciplinary action being taken.

All monitoring information will be kept for six months.

## 17. Private Use

17.1 recognise their responsibility to maintain the privacy of individuals, comply with current legislation and the expectations of the School.

17.2 IT resources and facilities (including laptops provided to employees) are provided for School business purposes. Reasonable and responsible personal use is allowed, provided there is no conflict with the interests or requirements of the School. The School does not accept liability for any personal loss or damage incurred through using the resources and facilities for private use. The security of private information and data is the responsibility of the user.

17.3 In order to comply with the HM Revenue & Customs regulations on taxable benefits any use of a School laptop for an employee's private purposes must not be 'significant'.

## 18. Disciplinary and Related Action

18.1 Suspected misuse of the School's computer systems by a member of staff will be considered by the Head Teacher. Failure to follow the IT Acceptable Use Policy could result in disciplinary action being taken and include a

warning, suspension, dismissal from the School and in the case of illegal activities referral to the Police.

## 19. Summary

19.1 School managers have a duty of care to all staff and to ensure that they have a reasonable work-life balance and that they are able to work in a healthy and safe environment. Headteachers should therefore try to ensure that electronic working does not place greater burdens on staff in terms of either workload or response times. Headteachers should also endeavour to support any staff who are subject to abuse through any of the electronic media, by effective and immediate sanctions, in the same way with which it is expected verbal and physical abuse would be dealt.

19.2 Staff should always be reminded to think carefully about all forms of communication, but particularly electronic methods (which can be circulated widely and rapidly). If 'thinking about it' gives rise to any doubt, then the best advice is 'don't do it'.

19.3 This is a rapidly changing and developing area. This guidance provides initial advice, of which all staff should be made aware. It is anticipated however that it will be reviewed and updated regularly in the light of technological changes.

**ACCEPTABLE USE AGREEMENT - STAFF**

**DECLARATION**

I confirm that I have received appropriate training, read and understood the School Staff IT Acceptable Use policy on the use of IT resources.

Name: (please print)

Signed:

Date:

**ACCEPTABLE USE AGREEMENT – STAFF**

**SCHOOL LAPTOP EQUIPMENT & SOFTWARE**

| Hardware Details | Date Issued |
|---|---|
| Laptop model | |
| Laptop Serial number | |
| Laptop bag & Manuals | |

| Software Details | Installed |
|---|---|
| Microsoft Windows 7 | |
| Microsoft Office 2010 | |
| Anti-Virus software | |
| Additional software as required | |
| Additional software as required | |
| Additional software as required | |
| Additional software as required | |
| Additional software as required | |

**DECLARATION**

I confirm that I have received the equipment and software as specified above and understand the terms and conditions of use as set out in the above School Staff IT Acceptable Use.

Name: (please print)

Signed:

Date:

## APPENDIX 1

## Employee Guidance on the Use of Social Media

- Staff must be mindful that any online activities/comments made in a public domain, must be compatible with their position within the School, and safeguard themselves in a professional capacity.

- Protect your own privacy. To ensure that your social network account does not compromise your professional position, ensure that your privacy settings are set correctly. Remember to upgrade access settings whenever the application/programme is upgraded.

- When setting up your profile online consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details. Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be "private" may still be in contravention of the Employee Code of Conduct, the Harassment and Bullying Policy and/or the Disciplinary Policy. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.

- Do not discuss work-related issues online, including conversations about pupils, parents, complaints, management or disparaging remarks about colleagues or the School. Even when anonymised, these are likely to be inappropriate. In addition doing this in the presence of others may be deemed as bullying and/or harassment.

- Do not under any circumstances accept friend requests from a person you believe could be a 'service user' or may conflict with your employment.

- Be aware that other users may access your profile and if they find the information and/or images it contains offensive, make a complaint about you to the School as your employer.

- Ensure that any comments and/or images cannot be deemed defamatory, libelous or in breach of copyright legislation.

- You can take action if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others.

- If you do find inappropriate references and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. It is wise to alert your friends in advance to the implications for you, as a school employee, of posting material related to you.

- If you find inappropriate references to you posted by parents, colleagues, pupils or other members of the school community, report this to the Headteacher.

- If you are very concerned about someone else's behaviour online, you should take steps to raise your concerns. If these are work related you should inform your manager.

- Staff should also act in accordance with the School's Code of Conduct, Policy on the Acceptable use of IT, the Internet and Electronic Communication, Safeguarding Policy and Harassment and Bullying Policy.

- Staff should not access social media sites or leave these running in the background during working time, on any devices within their control.

## APPENDIX 2

## Additional Guidance for Headteachers on the Use of Social Media

**Headteachers have a responsibility to:**

- Remain familiar with this policy and the employee guidelines to using social media included in the Appendix.
- Ensure staff are made aware of the policy, employee guidelines and provided with appropriate training/briefing.
- Take prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not, including taking steps to seek the prompt removal of any inappropriate material.
- Make parents and pupils aware of the implications of posting comments about the school and members of its community. Details will be included in the Home School Agreement and/or school brochure, to indicate the appropriate means for parents of raising any concerns. It is advised that these documents also make reference to the potential implications of posting inappropriate comments about the school/staff/pupils/wider community members. The agreement will also warn against the taking of unauthorised photgraphs of staff and/or making sound recordings.
- Support employees who are the subject of abuse, through existing policies and procedures.
- Ensure all complaints/allegations are dealt with fairly and consistently, and in accordance with other employment policies where appropriate.

**Headteachers are advised to:**

- Ensure staff are advised of this policy on appointment and discussion and elaboration is included during induction such that they are fully aware of its content.
- Remind staff on an annual basis of the guidance on use of social media.
- Ensure staff are aware of how to raise concerns
- Include in the relevant section of the Information and Communication Technology curriculum, advice for pupils on the safe use of social media, the restrictions on use of these media for contact with school staff and the implications of posting material on such sites.
- Provide guidance for parents in supporting their children's safe use of social media
- Include in documents like the school brochure and home/school agreement the school's approach to the taking of photographs of pupils, by the school or by parents, and how these may be used. Seeking parents' agreement at the outset and alerting them to potential pitfalls is likely to reduce issues of concern occurring. Parents may need to be made aware of the potential consequences of posting pictures on social media which include children other than their own, without parents' permission.
- Ensure parents and pupils are made aware that the use of social media to make inappropriate comments about staff, other parents or pupils will be addressed by the school in the same way as if these remarks were made in person, in the public domain.

- Seek the advice of the local authority if experiencing difficulty in securing the removal of inappropriate material from a site or, in serious cases, for legal advice concerning the content of what has been posted.

**Definition of 'libel' and 'defamation'**

Any comments or statements made online may be viewed as defamatory/libellous and members of the school community need to be aware that they may be also be held accountable for comments made online in a court of law.
Defamation is the act of making a statement about a person or company that is considered to harm their reputation, and may cause actual loss/costs to the person/company. If the defamation is written down (print or online) this is known as libel.