

 <p>Cotmanhay Infant and Nursery School</p>	<h2 style="margin: 0;">Acceptable Use of IT, the Internet and Electronic Communication Policy</h2>		
	<input type="checkbox"/> Complete Revision <input checked="" type="checkbox"/> Partial Revision <input type="checkbox"/> New <input type="checkbox"/> No changes	Review cycle: Annual	Pages: 28

Author of the policy:

<input checked="" type="checkbox"/> Derbyshire County Council	<input type="checkbox"/> School based	<input type="checkbox"/> Other
	Name:	Details:

If Derbyshire County Council / DfE, which issue number:

Issue 1	Issue 2	Issue 3	Issue 4	Issue 5	Issue 6	Issue 7	Issue 8	Issue 9	Issue 10
Nov 19	April 20	Nov 2022	Dec 2023	April 2024					

REVISION RECORD:

Review date	Revised by	Comments
Feb 19	K Gillott	New guidelines
Nov 19	K Gillott	Data retention update 14.4 use amended 13.6
April 2020	K Gillott	Teams update 20.4.2020
Nov 2022	K Gillott	Update to teams section and omitted section from parent appendix 11.11.22
December 2023	K Gillott/S Meer	Updated in line with the KCSIE updates and removal of use of memory sticks.
April 2024	S Meer	Updated to include mobile phones can be used in class or on trips for educational purposes and adding to dojo. Page 16

We are committed to safeguarding and promoting the welfare of children and young people and expect all staff and volunteers to share this commitment.

Acceptable Use of IT, the Internet and Electronic Communication Policy

Cotmanhay Infant and Nursery School



CONTENTS

Introduction

Scope

Use of Internet, Email and other Electronic Communication

Safe Working Practice

Virtual Learning Environment

Microsoft Teams

Social Media

Safeguarding

Newly Qualified Staff

Laptops issued to Staff

Health and Safety guidance on using IT equipment including Laptops

Use of other School IT Equipment

Software

Network Access, Passwords and Data Security

Encryption

Monitoring of Email

Monitoring Internet Access and Instant Messages

Private Use

Disciplinary and Related Action

Summary

Acceptable Use Agreement

Appendix 1- Additional Guidance for Headteachers on the use of Social Media

Section 1: Introduction

Purpose:

The Acceptable Use Policy (AUP) is an addendum to the school's general computing Policy. It addresses issues related to the acceptable use of the ICT facilities provided for pupils, staff, parents and governors to use. 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.

Aim(s):

- To safeguard individuals from offensive messages, personal or impersonal, in any medium capable of being held on a computer system, e.g. malicious e-mails, messages, pornographic images, AI misuse, sexting, cyber-bullying etc.
- Safeguards the anonymity of pupils and their computer-based work, including social media sites when that is appropriate.
- Safeguards the integrity of computer-based information held within the school or on behalf of the school.
- Safeguards the good standing and legal integrity of the school in terms of computer-based information that is held publicly.

Wider school aims/ethos:

This policy supports our school aim of safeguarding and promoting the welfare of all pupils.

Consultation:

K Gillott, senior leader and S Meer, computing leader wrote this policy.

In consultation with:

- **Staff**- during staff development and key safeguarding meetings.
- **Pupils**- completing a classroom agreement to accept and follow the e-safety golden rules.
- **Parents**- during inductions and updates to parents via the website and newsletters.
- **Governors**- full governing body meeting.

Updated in relation to the Acceptable Use of the internet and Electronic mail Derbyshire policy.

Section 2: Scope

- 2.1 This policy applies to all technology and communications equipment provided by Cotmanhay Infant School (e.g PCs, laptops, mobile phones, iPads with Internet access etc).
- 2.2 Any personal or potentially personal information sent via e-mail and the Internet is covered by GDPR 2018. 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 correspondence that is more formal.
- 2.4 Use of e-mail and the Internet, which brings the school into disrepute, may result in disciplinary action.
- 2.5 Use of the Internet and e-mail is permitted, subject to these principles:
 - a. E-mail: Employees must only use school e-mail for professional 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 is permitted subject to these principles and guidance notes.

Email

- 3.1 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 non-teaching times.
- 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 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 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 always follow school protocol and 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.

- 3.4.1 Staff using email on a school device such as iPad or laptop, should only do so through Safari, Chrome, Edge or the Outlook app. Staff should always log out after reading emails on laptops or PCS for data protection purposes. iPads are password protected therefore logging out is not necessary.
 - 3.4.2 If staff are using email on their phones, this must be protected by a password known only by themselves and this must not be shared with anybody else. If it is likely that anyone could access your email application, then you must use an internet-based engine to read and check emails that can be logged out of.
 - 3.4.3 **Two-factor authentication** must be enabled on school email systems for security reasons.
- 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, which for Cotmanhay Infant and Nursery is to encrypt the email. 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 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.

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. Any material that is deemed inappropriate must be recorded in the cyber log book located in the staffroom or on the QR code attached to the weekly newsletter and reported to the computing lead / IT technician. 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 downloaded 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 login 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 by using the windows L button when they leave a room.
- 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. **No apps or programs should be installed without the IT technician adding them to the apple management system, even free apps.**

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. All content to be shown to students must be checked beforehand.

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 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 purple mash, 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. Microsoft Teams

Teams is now used within our school setting for meetings which are no longer face to face such as conferences, courses and governor/safeguarding meetings. Whilst this is a valuable tool, we need to ensure that we are safeguarding everyone's privacy. (GDPR)

Microsoft Teams will be used for Staff and Governors using school email addresses generated by the school only and for communication with other school staff and conferences or courses that cannot be held in person.

We will not be recording and holding any data from any of the meetings within Microsoft teams and will use it only to collaborate information and communicate.

Teams will not be used as an online platform for lessons to pupils nor to communicate with parents unless it is safeguarding meeting held with a team of professionals.

All staff members must ensure that the data is protected and privacy is maintained during any online meeting using Microsoft teams. If this is unable to happen the meeting should be postponed until data and privacy can be protected.

7. Social Media (This now supersedes the old Social media policy)

Some of the content in section 6 utilises and builds on the ***Kent County Council/The Education People online safety policy template***, with their permission.)

7.1 **Definitions:**

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, Instagram, Snapchat, LinkedIn, internet newsgroups, blogs, wikis, bulletin boards, video/photo sharing sites and chatrooms, Whats App. Social media also covers blogs and video-and image-sharing websites such as YouTube, TikTok 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. This policy applies to the misuse of social media for both business and personal purposes, whether during working hours or otherwise.

The use of sites such as Facebook, Messenger, Twitter, TikTok 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.)

'Libel' and 'Defamation'

Libel and Defamation are complex areas of law. Legal advice should be sought where Libel and/or Defamation are believed to have occurred.

7.2 Personal Safety and Protection:

At all times, staff should be aware of the school's expectations, as defined in all relevant policies, of professional adults working with children. Safe and responsible use of social media will be discussed with all members of staff as part of induction and revisited regularly. This document describes safe and professional behaviour in relation to social media. **Headteachers can now use a search engine and social media sites, to research a candidate before employment.**

Online conduct can have an impact on the role and reputation of staff members. 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.

Staff are advised to safeguard themselves and their privacy when using social media sites. Areas of which to be mindful:-

- Setting the privacy levels of personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Not representing personal views as those of the school.

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. Staff are advised not to communicate, or add as 'friends' any past learners **or their family members** via social media sites. 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 use school platforms only to communicate with pupils, in line with the Safeguarding Policy.

Staff should report any inappropriate contact from pupils and parents/carers to a member of the Senior Leadership Team at the earliest opportunity to prevent situations from escalating. *(See paragraph 6.9 for support for staff.)*

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. It is expected that such exceptions will be discussed with the Headteacher.

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.

7.3 Personal Accountability and Responsibility:

All staff 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 Staff 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.

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.

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.

The School views any comment that is made on social media to, potentially, have been made publicly. However, any inappropriate comment will be considered in the context in which it is made. Members of staff should inform the Headteacher if they consider any content shared on a social media site potentially conflicts with their role.

Staff should be aware that all comments made through social media must meet the standards of the relevant legislation and regulations, including data protection

legislation (GDPR 2018) and the expectations of staff conduct as expressed in the school's policies for the management of Human Resources.

7.4 Any Communications that staff 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 or sharing confidential information, including photographs and personal information about individuals (such as pupils, their family members or colleagues) 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 member of the school community (such as an employee of the School, 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 Harassment and Bullying policy, or the Equality and Diversity Policy.

While use of the school's facilities to express personal views is inappropriate and unacceptable, it is recognised that individuals have a right to enter general political discourse, using their own accounts and in non-working time. It would still be important to make it clear that a personal view is being expressed and any extreme statements, as listed above, would contravene this policy.

The above bulleted examples are not a definitive list of the misuse of social media, but are examples to illustrate what misuse may look like. Staff are encouraged to talk to their Headteacher and seek advice if they are unclear.

7.5 Official Use of Social Media

Staff who use social media as part of their job must adhere to the school policy. Employees must be aware that they are representing the school and use the same safeguards as they would with any other form of communication about the organisation in the public domain.

- Cotmanhay Infant and Nursery official social media channels are:
 - *Classdojo* <https://home.classdojo.com>
 - *Twitter* <https://twitter.com/CotInfants>
 - *Facebook* <https://www.facebook.com/Cotmanhay-Infants-373805669459385/> .
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the *Headteacher*.
 - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use setting provided email addresses to register for and manage any official social media channels. info@cotmanhay-inf.derbyshire.sch.uk
 - Official social media sites are suitably protected and, where possible, are linked to our website.
 - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
 - Only social media tools which have been risk assessed and approved as suitable for educational purposes, will be used.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude other methods of communication, so as to reach any members of the community who are unable or unwilling

to utilise social media. Consideration will be given to the universality of any form of communication utilised.

There should be no expectation that either staff or pupils will be available outside normal school hours. If schools are to utilise this, Headteachers should ensure that a reasonable level of monitoring is in place, to prevent any inappropriate comments or 'cyber-bullying', and ensure that pupils know that such monitoring is taking place.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
 - Sign our social media acceptable use policy.
 - Always be professional and aware they are an ambassador for the setting.
 - Disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the setting.
 - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
 - Ensure that they have appropriate consent before sharing images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - Inform the Headteacher of any concerns, such as criticism, inappropriate content or contact from parents.

Many social media complaints arise out of parental frustrations and because parents may feel that they are not listened to or valued by schools and may set up unofficial and unapproved Facebook pages or groups. In some cases, Facebook pages or groups may be set up and run via parent teacher associations or other similar groups. The school Facebook page is for information sharing only and the comments facility is disabled.

7.6 Access to Social Media at Work, for Personal Use:

Staff are not allowed to access social media websites for personal use from the school's computers or devices during working hours (contact time for teachers and teaching assistants), and they must not be left running "in the background", whilst at work.

Leaving social media sites 'running' constantly in work's time is considered to be a breach of the acceptable use of this 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. These provisions also apply to personal computers and mobile devices.

7.7 Use of Personal Devices and Mobile Phones

Cotmanhay Infant and Nursery School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

7.8 Expectations

All use of personal devices (including but not limited to; tablets, game consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

- All members of the Cotmanhay infant and Nursery School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of the Cotmanhay infant and Nursery School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices, is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of the Cotmanhay infant and Nursery School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe place during lesson times.
- Keep mobile phones and personal devices switched to 'silent' mode during lesson times.
- Not use personal devices during teaching periods, unless it has a positive impact on the learning or in emergency circumstances.
- Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers, unless the individual can withhold their number. Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher.

- Staff may use personal devices to take photos or videos of pupils if it is for an educational purpose, for school-based outings or adding to the dojo page. All images must be removed before leaving the school site.
- If a member of staff breaches our policy, action will be taken in line with relevant school policies. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

7.9i Responding to Online safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.

Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure. We require staff, parents, carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. We will refer to the flowchart on responding to incidents, made available. Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Headteacher will speak with Call Derbyshire.

7.9ii Dealing with Inappropriate References to the School or Staff

Members of staff who find that 'friends' have posted inappropriate material, relating to themselves on a social media site should consider asking them and the site to remove it. Also consider informing the Headteacher if there is the potential for repercussions for the organisation.

If you find yourself the target of complaints or abuse on social networking sites you can take action yourself by using the mechanisms to report abusive activity. Most sites also provide some support for users who are subject to abuse. Again, it is advisable to let the Headteacher know so you can benefit from their support.

If you find inappropriate references to you or the school posted by parents, colleagues, pupils or other members of the community, it is very important that you report this to the Headteacher as soon as possible. Do not attempt to address the situation yourself. The Headteacher will then respond to the situation and ascertain your support needs.

See Appendix 1

8. Safeguarding

- 8.1 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.

The Headteacher will however need to give consideration to a procedure for a staff member receiving a disclosure from a pupil outside the normal working day. Schools will need to determine their own best response to such a situation and ensure that all staff are fully aware of the procedure as part of their regular safeguarding training.

School administrators may wish to consider an auto response email system providing contact numbers (e.g. social services) for out-of-hours emergencies.

9. Newly Qualified Staff

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. 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.

10. Laptops/iPads issued to staff

- 10.1 The laptop/ iPad remains the **property of the School** and is provided to users on a loaned basis. The laptop/iPad 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/iPad should not be removed for any reason.
- 10.2 School laptops/ iPads 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.
- 10.3 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 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.
- 10.4 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/iPad will then be securely deleted.

- 10.5 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.
- a. 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/iPad whilst on loan.

11. Health and Safety guidance on using IT equipment including laptops

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.

12. Use of other School IT Equipment

12.1 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.

12.2 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.

13. Software

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).

14 Network Access, Passwords and Data Security

14.1 Users must only access information held on the School's computer systems if properly authorised 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.

14.2 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. All staff must log out of the computer as soon as they have finished and must not leave a computer unattended. Pupils should always be logged on as themselves.

14.3 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, staff will be prompted for this. System and administration level passwords should also be changed, at least on a termly basis.

14.4 All passwords are to be treated as sensitive, confidential information. Cyber security training strongly recommends that staff do 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.

14.5 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.

14.6 The Administrator of each system will check passwords and access controls annually to ensure any old users are removed.

15. Encryption

15.1 Sensitive or confidential information held on laptops or other portable device 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.

- 15.2 All data that is sensitive **MUST** be treated in the same regard as school records. It is the individual's personal responsibility for records or data stored on the cloud, on email or on ipads/laptops in their possession when onsite and off-site. When pupils have left the school ALL old data must either be deleted or where necessary shared with the new school. (Apart from First Aid data)
- 15.3 All members of staff need to check the school's network on an **annual basis** and ensure that any data stored is in line with the data protection policy and the school's data retention policy. It is staff members individual responsibility to check their own folders and ensure there is no breach of data.
- 15.4 All members of staff need to carry out annual housekeeping at the end of each academic year and remove any data in line with the schools Records Retention Policy.

16. Monitoring of email

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 Head teacher. 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 Head teacher. The Head teacher 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.

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.

17. Private Use

- 17.1 Staff should 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

Suspected misuse of the School's computer systems by a member of staff will be considered by the Head Teacher. Failure to follow the 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. Head teachers 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.

Main Points for Staff to Remember

- Do not divulge your staff logon password under any circumstances and change it if you think it has been compromised.
- Do not leave a computer unattended and logged on to a staff logon.
- Explicitly teach pupils the points laid out in the e-mail section above when relevant e-mail activities are about to begin.
- Explicitly teach online safety to the pupils and display the online safety poster near the computers so that the pupils can refer to it at any moment in time.
- Ensure that all pupils follow the same procedures for things found or seen that they do not like, switch off the screen, tell someone.
- Actively monitor the websites that pupils are visiting before they use the page themselves and do not leave a group unsupervised.
- Try wherever possible to visit websites before you use them in your teaching so that you can check their acceptability.
- Report any inappropriate websites that you find to the computing lead/IT technician so that they can be filtered out.
- Always respond to an on-screen virus warning. Isolate the machine and inform the computing lead/IT technician immediately.
- Use one drive or share point to save data on.
- Never open or execute a file sent to you by someone that you don't know. Delete it immediately and report in all circumstances.
- Do not buy or sell anything via the school network without the permission of the head teacher.
- Do not access social media for personal use during your working day.
- Connect to Guest Wi-Fi.
- Adhere to the social media policy.
- Never look at an image that may be inappropriate, inform the Head Teacher and DSL (designated safeguard lead) immediately.
- Microsoft teams to be used only using the school email address during meetings. Staff must ensure that the correct privacy is adhered to during these calls.

Teaching Points for Pupils

- Keep your passwords safe
- Do not log on as anyone else without their permission.
- If you get a message on the screen about a virus, stop working and tell a teacher straight away.
- Do not put memory sticks or CDs into the school's computers.
- If you see anything on the Internet that you think is upsetting or rude, switch off the screen and show it to a teacher straight away. Ensure that you always tell someone, even you have seen something on someone's phone or mobile device.
- Do not give your e-mail address to anybody, particularly a stranger, without asking your teacher first.
- Never type your name, address or other personal details in on a web page without asking permission first.
- If you receive an e-mail from somebody that you don't know, tell a teacher immediately.
- Never tell anyone private details about yourself in an e-mail, especially your address and telephone number.
- Remember that the school rules about being kind and considerate in what we say to others, applies to social media and gaming as well.
- Be aware that e-mail is not private and that teachers will see what you have written.
- Be aware that the network can detect misuse of the computers and record details of the person responsible.
- Never download files or programs from the Internet.
- Tell a teacher about any files attached to an e-mail that you were not expecting to receive.

Main Points for parents to remember

- The school wishes to remind its parents that Social Media sites are only intended for users **aged over 13**.
- Social media must not be used for interactions between teachers and pupils or teachers and parents.
- Social media must not be used to hold inappropriate communications or inappropriate postings that involve other pupils, staff members or the school itself.
- Social media must not be used to publish unpleasant or abusive postings about teachers or pupils or any photos of pupils other than your own.
- Social media must not be used to criticise the school (not personally abusive).
- The setting up of fake profiles is prohibited and against all social media policy.
- If you do have any online safety concerns regarding your own child or yourself please always speak to a member of staff who will support you.

Any form of misuse directed at the school, its employees, the pupils or anyone associated with the school will be taken very seriously. If any illegal activity or content is suspected the school will inform the necessary authorities.

Parents and staff members are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Data will be processed in line with the requirements and protections set out in the General Data Protection Regulation.

Appendix 1

Advice for Headteachers – Introduction

In some cases, parents have bypassed the school's complaints procedures and taken to social networking sites to criticise and, in some cases, make malicious comments about individual members of staff or the community or regarding decisions that have been taken by the Headteacher.

In many ways the use of social networking sites to express these opinions is an extension of how people can already express their views on the internet. People use sites to review holiday accommodation and give assessments of products they have purchased. However, remarks made about a school, member of staff or child can be destabilising for a community and, in particular, for the professional status of staff members who may have had allegations made against them and the emotional well-being of children and young people who may have been identified. It can also lead to a 'whispering campaign' which can undermine the school leadership or target a particular child or family.

There is no single effective method of dealing with parents, carers, pupils or others who raise issues on social networking sites. However, schools can take a proactive approach to minimise such incidents rather than having to be reactive and put together a quick response to stop the spread of rumours. This guidance gives a number of approaches educational settings can use to deal with any problems as well as preventative approaches to help ensure that parents and carers follow the appropriate complaints procedure in the school.

Preventative Actions

Headteachers should seek to minimize the potential for parents, carers, pupils and others to post comments about the school and members of its community by setting out the implications in any relevant documentation, like the Home School Agreement and school brochure.

While it is difficult to monitor all parents' use of social networking sites, it does show that the school takes this matter seriously and, the fact that parents have signed the agreement, means that they have a responsibility to act appropriately. Although the expectations of pupils not to misuse social media will be contained in other school policies it would be wise to include a reference in the Home School Agreement. It is important to include information about the appropriate means of raising concerns and the schools commitment to working co-operatively with parents. The complaints policy should be highlighted and easily accessible via the school's website. Headteachers may also wish to draw attention to other related policies including anti-bullying, Safeguarding, online safety, data protection/security and confidentiality. 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 implications will include the detrimental effect on individuals, the reputation of the school and subsequent potential for the focus on children's learning to be impaired.

It should be made clear that the school will not tolerate abuse of staff, and will take any appropriate action. Schools may also wish to remind parents that they can "report" any unpleasant comments or content to Facebook or other social networking sites, who may remove comments and block/ban users who break these rules. Parents should also be aware of the importance of role modelling appropriate behaviour for their children online, much like they should offline. The use of social media should also be included in meetings for new parents, where it can be linked to the schools efforts to also protect children from cyber bullying.

Headteachers may want to consider implementing a range of routes to encourage parents to raise concerns directly with the school, for example ensuring a senior member of staff is available on the gate at the start and end of the school day, dedicated email accounts etc.

Leaders should ensure that all members of staff receive safeguarding training that is robust and up-to-date and covers online safety (as identified within 'Keeping Children Safe in Education' 2023). This training should include ensuring that all members of staff know how to respond to concerns they may see online in a way that supports the school and also does not compromise them.

Responding to Specific Concerns

It is important to acknowledge that each situation will be different and there may be various complicating factors which need to be taken into account.

However the following steps may be applied where appropriate:-

a) *Keep calm*

Although sometimes difficult, it is essential that leaders ensure that their response to comments posted on social media is proportionate and impartial. A measured response is more likely to promote a positive outcome.

b) *Gather Evidence*

It is important that any evidence is kept to enable schools to collate a record of events; this should include usernames, specific dates and times, as well as actions taken by the school. In many situations this will be a one-off concern which can be resolved quickly, however in some situations this could be part of a bigger or ongoing issue; therefore, a clear chronology will be helpful.

Where the Headteacher becomes aware of the posting of negative comments it is important to gather evidence (such as screen shots and print-outs, including times, dates and names where possible and ensuring the identity of the person who reported the issue is removed) and establish exactly what has been posted. This may have to be done through various methods as the information may have only been shared through the connections of specific people. However, it is important that evidence be submitted so that the facts can be established. Headteachers need to be very careful when utilising such material; that it is not shared inappropriately and confidentiality is maintained. When dealing with cases involving Facebook, a group of parents may have set up a site or closed/secret group to comment about or, in some cases, criticise the school or individual members of staff.

It is important that members of staff do not become embroiled in entering the discussion. The social media site is a public forum and anything written by the school can be utilised by the media or other interested party and may be misinterpreted or used for their own agenda. This advice is also applicable to the school's own social media platform; however, it is a good idea to exercise the rites of the site administrator and remove unacceptable material. If the author is known the school can then make contact to address any issue through the normal communication channels. It is helpful if the school can monitor the 'feed' during weekends and holidays as otherwise inappropriate remarks could remain for longer than necessary.

c) *Reassuring Those Affected*

If individual members of staff have been targeted or mentioned, then Headteachers will need to be mindful of their duty of care to those involved as there is a specific duty on employers to protect their staff from third party harassment. Appropriate support will depend on the nature of the concerns and the reaction of the individual. If the member of staff is already aware of the comments, then Headteachers should explain to them how they intend to address the concerns and offer support to them. Headteachers should encourage staff to let them know if there is any further support that they feel they need.

- Staff may wish to contact their professional/teaching union for additional support and guidance or access support via the Education Support Network: www.educationsupportpartnership.org.uk
- Staff and Headteachers can also access help via the Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- The school may also want to take further advice on this issue from their HR provider. If an allegation has been made then Headteachers will need to speak with the LADO.

If the member of staff is unaware of the comments, then Headteachers should consider if it is necessary to inform them, and if so, what would be the best approach. Headteachers are advised to discuss this with their HR provider, in the first instance.

d) *Meet with the Parents/Carers/Person Involved*

Headteachers should contact the person concerned and invite them to a meeting to discuss any concerns they have. (Any member of staff who is the subject of the posts will not be asked to attend.) Demonstrating that such issues will be taken seriously, if properly raised, should serve to show that there is no need to express their concerns in such an inappropriate way. It may be that the reason why a parent or carer has made the comments online is due to being oblivious about the implications of doing so or because they are unaware of, or disillusioned with, the school's complaints procedure. An immediate response in writing can occasionally inflame situations (and indeed in some cases ends up being shared on social media itself) so a face to face or "offline" discussion is likely to have a more positive outcome. If multiple parents are involved then schools should consider how best to respond safely and effectively, whilst maintaining confidentiality. This may require multiple individual meetings with parents.

In these circumstances, the Headteacher is advised to be accompanied by a suitable leadership team colleague to express their disappointment with the current situation and explain that the school would like to work with them to resolve the problem that is obviously causing them distress. Headteachers should explain how this behaviour can have a detrimental impact on the school and potentially their children's education, while not allowing the school to actually address their concerns. At this stage, the Headteacher should request that any offending posts or pages are immediately removed and encourage the parents to work with the school. If appropriate, they can be signposted to the School Complaints procedure or other process to raise any relevant concerns they have regarding the school and its employees.

Parents should be made aware that comments posed online (even if made "privately") can easily be misread or misinterpreted and can also be shared without their knowledge or consent. Although it is essential not to cause any further problems, the professional status of staff and the school needs to be maintained and it cannot be compromised by any malicious comments or allegations. The

school may want to warn the parents that any existing comments or a continuation of posts could lead to civil or criminal action being taken, although the school would prefer to avoid having to take this route.

If Headteachers think that a criminal offence has been committed, or believe that speaking directly to the parents would lead to a confrontation or offence being committed, then they should contact their Local Police contact to work together to support the school in discussing this with the parent concerned.

Where there are a number of parties exchanging comments and where the school has been informed that negative comments are being made but cannot view the thread, then it is recommended that a general letter to parents is considered reminding them of the detrimental effect on individuals, including pupils, and the school itself that posting negative and unsubstantiated comments may have. Parents can be reminded of the ease of approaching the school with any concerns and the appropriate channels for raising complaints.

Schools are strongly advised to contact the LA's public relations' 'Crisis Communications Team' to let them know of any inappropriate comments posted on social media, as journalists monitor accessible sites and will often contact the Authority about an issue they have picked up. It is very helpful for the team to be alerted to the situation and be ready to respond to any enquiries from the media. Those schools purchasing the traded service can access support in drafting a statement to be used, if necessary.

Resolving Difficult Situations

Where the school's actions have been unable to resolve the situation, to ensure that the parents understand the seriousness of the matter, a further meeting should be arranged, with the chair of governors present, to convey the damage that these comments are having on the school community. It is essential that the chair of governors is fully briefed before the meeting and that a common approach is taken by the school to address this matter. Again, it gives an opportunity for the parents to share any grievances and for an action plan to be established to deal with any concerns expressed by them. If parents refuse to meet with the school, then the Headteacher/chair of governors may wish to send a letter, after taking advice from LA Legal Services (or other provider). The legislation providing grounds for challenging offensive posts on social media is complex and the composition of any communication sent to the individual(s) concerned needs to be considered on a case by case basis. (see 4th Bullet point below)

The Local Authority understands how upsetting the posting of critical, offensive and even threatening comments on social media can be. While headteachers will support members of staff during such situations, they may also need support themselves.

- Any threats of violence should be reported to the police and they should also be informed of any comments that could cause serious harassment, alarm or distress. Again, contact could be made with the local police liaison officer about whether there is the potential for harassment proceedings or whether any other offences have been committed, although the case may be categorised as a civil matter.
 - Comments that are threatening, discriminatory, offensive, abusive or use foul language should be reported to the social media site with the request for them to be taken down. It is helpful to quote the site's own terms & conditions, highlighting where the remarks breach their policy. There is usually a button on the site to make such reports. Schools have to be aware that there will be a time delay in the review of this content and that if the content does not breach the terms and conditions, then the site administrators will not remove it.

Forced removal of comments may only occur if the comments break the law or break the website's terms and conditions.

- It is advised that the Headteacher's response to the comments also takes into account how widely the remarks are published and whether there is some truth in the content, however inappropriately expressed.
- Those purchasing the LA Legal Service can obtain legal advice on specific individual cases, or on the phrasing of any general letter (or relevant section of a document). Where appropriate, Legal Services will advise the school on the composition of a letter to the individual posting the comments. They have drafts on file ready for adaptation to the school's particular situation.
- For headteachers serving in Maintained Schools the LA has a duty of care and speaking to the school's designated adviser may be the first contact in seeking support to tackle the issue. The adviser will also signpost relevant sources of support available.

The following traded services are available for help and advice as appropriate:

- LA Legal Services
- LA Public Relations 'Crisis Communications Team'
- Local Authority Occupational health can provide a link to a counselling service
- The school's HR provider is a good source of advice
- Headteachers may wish to discuss with their school's School Improvement Adviser.

Other sources of support include:

- The Education Support Partnership is available online
- Many colleagues belong to a professional association, through which specific advice and general welfare support can be accessed
- Staff and Headteachers can also access help via the Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Childnet Teacher Guidance: www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- The Department for Education Preventing and Tackling Bullying (November 2014) www.gov.uk/government/publications/preventing-and-tackling-bullying