



DERBYSHIRE TRUST

Acceptable Use of IT Advice and Guidance

Date Last Updated	Confirmed Current
June 2023	Sept. 2024

FOREWORD

This new document has been the subject of formal negotiation and consultation with the recognised Trade Unions and Professional Associations and was agreed and adopted by the Schools' Joint Consultative Committee. Agreement and adoption was only reached by Schools Joint Consultative Committee where it is used in conjunction with the DCC Education Data Hub Policies. ACE Derbyshire Trust have chosen to formally adopt this policy.

This guidance has been developed to support the Trust's data protection and cyber security policies.

Derbyshire County Council's Education Data Hub Policies in this regard are:

- IT Security and Acceptable Use Policy
- Social Media Policy
- Bring Your Own Device Policy
- Off-site working policy

All schools are required to have policies on data protection and cyber security and this advice and guidance is designed to reflect the legislative requirements outlined in these policies whether they are purchased from Derbyshire Education Data Hub or elsewhere.

In combination the data protection and cyber security policies, along with this advice and guidance, provide the most up to date information about this rapidly changing area of responsibility for schools. It is necessary for schools to inform all staff and to make the document easily and freely available. Schools are advised that team meetings are used to remind staff of the provisions of their data protection and cyber security policies and this advice and guidance.

When adopting school's data protection and cyber security policies it is essential to follow the requirements set out in the Advice and Guidance which provides more context. Any school wishing or intending to adopt alternative advice and guidance must conduct its own formal consultations. It is also important to share the advice and guidance with staff and report any feedback received to the Trust.

August 2024

,

CONTENTS

1. Introduction
2. Scope & Definition
3. Email and other Electronic Communication
4. Acceptable Use
5. Recording Calls/ Meetings/ online lessons/ Staff Training
6. Copyright
7. Safe Working Practice
8. Virtual Learning Environment
9. Social Media
10. Disclosure over social media outside working hours
11. Induction of staff
12. Health and safety guidance on using IT devices
13. Network Access, Passwords and Data Security
14. Encryption
15. Monitoring
16. Disciplinary and Related Action
17. Summary

Acceptable Use Agreement – Staff

Appendices

Appendix 1 - Employee Guidance on the use of Social Media

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

1. Introduction

This document provides more detailed guidance to ACE Derbyshire Trust in respect of how the school is best able to respond to employment matters that arise in relation to staff's Use of IT and Electronic Communications.

This document forms the basis upon which the Schools' HR Advisory Service will best be able to offer support.

This guidance has been developed to support the following school's data protection and cyber security policies:

- IT security and Acceptable Use Policy
- Social Media Policy
- Bring Your Own Device Policy
- Off-site working Policy

Schools are expected to provide all of the IT resources necessary to enable staff to undertake their contractual duties and responsibilities. Staff will not normally be expected to use their own personal devices in order to fulfil their role.

2. Scope & Definition

This guidance applies to anyone working for the school, including permanent and temporary staff, volunteers, Governors and other Trust employees and representatives.

Where a member of the school community is referred to in this document, this is defined as including pupils, all employees of the school, volunteers helping at the school, supply and peripatetic staff, parents/carers and extended family members of pupils, Governors, individuals, and members of organisations providing a service to the school (e.g., sports coach, visitor invited to provide input to students).

3. Email and other Electronic Communication

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.

- 3.1 Staff should be aware that email is not always the best form of communication and should consider alternatives, as appropriate.
- 3.2 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.

4. Acceptable Use

Use of email and the Internet, which brings the Trust/school into disrepute, may result in disciplinary action.

Employees may receive an email 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.

5. Recording Calls/ Meetings/ online lessons/ Staff Training

Recordings should only be made using devices and software applications approved by the employer for this purpose.

Consideration should be given in advance as to whether it would be necessary and appropriate to record calls, meetings, online lessons. Schools should refer to their IT Security and Acceptable Use policy for more information.

Agreement to the recording must be obtained from all participants beforehand and participants should be made aware of purpose of the recording and their rights over their personal data. A person may not be recorded without their agreement.

A clear written process for recordings should be in place, which all those involved are aware of prior to recording, which addresses:

- Purpose of recording e.g. to support accurate minute taking;
- Lawful basis;
- Procedure for recording process;
- How agreement to record meeting/conversation will be recorded for all participants;
- Approved devices and software applications to be used;
- Communications regarding recording process with participants;
- Who the recording will be shared with;
- Categories of personal data being discussed;
- Technological and organisational measures to keep recording secure;
- Responsibilities of those involved in meeting/conversation;
- How long will recordings be kept and what will be the procedure for deleting them; and
- How rights of individuals being recorded will be met in compliance with data protection legislation e.g. process for making a subject access request in relation to recording.

Please note - video recordings of meetings or training sessions, in which individuals are not going to be identified will not require a data protection impact assessment. Any

such sessions to be recorded will require a clear written process, as described above, and all attending must agree to recording prior to meeting.

Recordings must not be made covertly. Staff should be reminded that there is an expectation that they will not record meetings.

School leaders are expected to embed an open and supportive school culture which enables staff to express any concerns that they have about being recorded openly. Staff must be given the opportunity to object to being recorded without fear of retribution.

6. Copyright

Employees may be in violation of copyright law if text is simply cut and pasted from any electronic media site into another document. This may equally apply to photographs, video, software, music samples, etc., 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.

7. Safe Working Practice

7.1 Staff are responsible for maintaining the security of computers. DfE cyber standards recommend:

- **securing your devices** **the logic behind 3 random words**
- **password managers**

Devices/machines should be locked when not in use.

7.2 Staff should ensure that when using work equipment at home, other family members do not use the equipment for their personal use. Software should be managed by the school IT. Staff should not have permission to download software as per DfE cyber standards.

7.3 Staff should not have access to install software on school devices.

7.4 Guidance from current KCSiE paragraph 141 states:

“Staff should have an awareness of the filtering and monitoring systems in place (Prevent Duty) and know how to escalate concerns when identified.” Please refer to your Safeguarding and Online Safety policies for further guidance.

8. Virtual Learning Environments (VLE)

8.1 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. Security and account access should be managed as outlined in section 12

- 8.2 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.
- 8.3 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.

9. Social Media

9.1 Definitions

There are many examples of social media. These guidelines should be followed in relation to any social media used. The social media policy and this guidance applies to the use of social media for both business and personal purposes, whether during working hours or otherwise.

9.2 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.

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 should ensure that there is no conflict of interest when linking through social media to people they also know through work. The school requires staff to only use school platforms to communicate with pupils, in line with the Safeguarding Policy.

Many staff will use social media 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 Designated Safeguarding Lead/Headteacher.

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.

9.3 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.

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.

The Headteacher and Trust 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 Headteacher/Trust will give consideration to whether the 'image' had been created voluntarily by the member of staff.

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.

9.4 Communications that staff make through social media:

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.

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;
 - 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.

The social media rules identified above 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/SLT manager and seek advice if they are unclear.

9.5 Official Use of Social Media

If schools are to utilise official social media sites 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. There should be no expectation that either staff or pupils will be available outside normal school hours.

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. ACE Derbyshire Trust advises that schools do not set up a Facebook page as the style of this platform could encourage the posting of informal comments and complaints. It may encourage the blurring of boundaries and appropriate channels of

communication. Also any editing of entries by the Headteacher could lead to challenge and allegations of bias.

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

Leaving social media sites 'running' constantly in work's time is considered to be a breach of the acceptable use of IT 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.

9.7 Expectations

- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, pupil toilets and swimming pools. (**List others in your setting as appropriate**)
- 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 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: (**Amend as appropriate**)

- Keep mobile phones and personal devices in a safe and secure place (**List details e.g. locked in a locker/drawer**) during lesson times.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Not use personal devices when engaged in lessons/learning (**Amend as appropriate**), unless written permission has been given by the *Headteacher/manager*, except in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Staff will not use personal devices:

- To take photos or videos of learners and will only use work-provided equipment for this purpose, unless authorised in writing by the Headteacher, for specific purposes.
- Directly with learners and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policies, 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.

9.8 Responding to Online safety Incidents and Concerns

In accordance with the latest Keeping Children Safe in Education 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.

Learners, 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 learners 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/manager* will speak with Call Derbyshire.

9.9. Dealing with Inappropriate References to the School Staff - Advice for Headteachers

9.9.1 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. The guidance below 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.

9.9.2 Preventative Actions

Headteachers should seek to minimise 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. *(See suggested paragraph below which schools may wish to adapt)*

It should be made clear that the school will not tolerate abuse of staff, as referenced in the notice displayed about behaviour on school premises (attached to Harassment and Bullying Policy), 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 the latest 'Keeping Children Safe in Education' document). 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.

9.9.3 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 make a referral to 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 Trust to let them know of any inappropriate comments posted on social media, as journalists monitor accessible sites and will often contact the Trust about an issue they have picked up. It is very helpful for the Trust to be alerted to the situation and be ready to respond to any enquiries from the media.

9.9.4 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 the Trust's Legal Services 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).

ACE Derbyshire Trust 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.
- The Trust can obtain legal advice on specific individual cases, or on the phrasing of any general letter (or relevant section of a document). Where appropriate, the Trust's Legal Services will advise the school on the composition of a letter to the individual posting the comments.
-
- For Headteachers, the Trust 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:

- The Trust's Legal Services
- Employee Assistance Programme
- The school's HR provider
- 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 (July 2017) www.gov.uk/government/publications/preventing-and-tackling-bullying

Suggested Section for Insertion in Home School Agreement or School Brochure

(To follow any reference in the document to the school's approach to pupils' use of social media and measures to avoid cyber bullying.)

The school is committed to working with parents to promote children's online safety and believes that, as adults, we have a responsibility to behave as role models in our own use of social media. Staff are subject to a policy and guidance concerning any use they make of such sites. We ask that parents, carers and other members of the school community also bear in mind their own approach to the use of social media as detailed in the school's Online Safety Policy. Further, we ask for parents and carers support in addressing any inappropriate use of digital communication devices by pupils in school.

As a school we strive to achieve the best for all children, however we recognise that on some occasions you may feel that we could have done better. We ask that careful thought is given to any posts concerning the school or individual members. We would be grateful if parents do not use social media to raise concerns or complaints but, instead, encourage you to come into school and speak to us so that we can understand and help to solve the problem. If you then feel that the issue has not been dealt with appropriately, we will provide you with the Complaints Procedure. It is all our interests to address issues without delay so that we can maintain the focus on children's welfare and learning.

It is easy to make an entry on a site 'in the heat of the moment' but once material is on the internet it is difficult to fully erase. Such comments can be damaging to the individual and their welfare as well as, potentially, the smooth running of the school. There has been much publicity in recent times detailing the harmful effects experienced by children and adults from the misuse of social media. 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.

(See notice in school referring to behaviour on school property). The Police will be informed and legal advice taken with respect to any comments that are threatening, discriminatory, offensive, abusive, use foul language or threaten violence.

Although it is rewarding to hear of positive descriptions of school experience, it is important to bear in mind that other individuals may not wish to be named and situations can be misinterpreted. There are also likely to be negative consequences of posting pictures on social media which include children other than your own, without parents' permission.

Our commitment to you is to put the pupils' interests first and to work in partnership with you in this endeavour. Your co-operation in relation to the use of social media would be greatly appreciated. Enabling us to deal with any issues of concern through the appropriate process will help to maintain the focus on the school's core purpose.

(See Appendix 1 for a summary of the guidance for staff members and for Headteachers)

10. Disclosure over social media outside working hours

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.

You should refer to the school's safeguarding policy for further advice

Headteachers will need to give consideration to a procedure for a staff member receiving a disclosure from a pupil outside the normal working day. It can be easily proved that the member of staff has received the disclosure and so it must be acted on as quickly as reasonably possible. 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.)

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

11. Induction of Staff

All staff should be made aware of the social media policies, expectations as an employee as part of their induction to avoid any conflict. E.g., A midday supervisor may fall foul of social media particularly if they within the school community.

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.

12. Health and Safety guidance on using IT devices

In the interests of health and safety, staff are advised to adhere to the recommendations for the safe use of the user's own device.

Schools should refer to the advice contained in the Health, Safety and Wellbeing policy on Display Screen Equipment including cloud-based networks. Any health and safety concerns associated with the use of laptops should be discussed with the Headteacher.

13. Network Access, Passwords and Data Security

13.1 Schools have a responsibility to ensure accounts and access are setup in line with the DfE cyber standards, they should work with their IT suppliers or Network Managers to ensure that. Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

13.2 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.

13.3 Staff have a responsibility not to disclose any personal or confidential data, and to report immediately if data is accidentally accessed or breached following the school's reporting process.

Staff using devices 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.

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

14. Encryption

All devices such laptops or other portable devices (e.g. memory sticks) which are used to store personal or confidential data should be encrypted as advised as an appropriate measure in UK GDPR. Use of such devices for the storage of data should be minimised

15. Monitoring

The school reserves the right to make appropriate arrangements to monitor, log record and access all e-mail 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. .

All monitoring of email information, internet access and instant messages will be kept for six months.

16. Disciplinary and Related Action

In the vast majority of cases, where electronic systems are not used carefully or appropriately, or when there is a data breach, it is not due to any intentional or malicious act by an individual staff member. Therefore it is not usual practice to sanction staff members following IT incidents; there would be a focus on supporting and retraining the staff member, for example by ensuring that staff are trained and understand how to use systems appropriately and carefully or by putting in place technical measures to ensure that incidents do not occur again.

However, suspected misuse of the School's computer systems by a member of staff will be considered by the Headteacher. Failure to follow the IT Security and Acceptable Use and associated policies and this guidance 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.

17. Summary

- 17.1 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.
- 17.2 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'.
- 17.3 This is a rapidly changing and developing area. This guidance provides initial advice, of which all staff should be made aware. It should be part of a suite of data protection and a cyber security policy that should be updated regularly to reflect the most up to date legislation in this area.

ACCEPTABLE USE AGREEMENT - STAFF

DECLARATION

I confirm that I have received appropriate training, read, and understood the following school's data protection and cyber security policies and supporting advice and guidance:

- IT security and Acceptable Use Policy
- Social Media Policy
- Bring Your Own Device Policy
- Off-site working policy

Name: (please print)

Signed:

Date:

ACCEPTABLE USE AGREEMENT – STAFF
SCHOOL LAPTOP EQUIPMENT & SOFTWARE

School to provide a list of hardware and software provided to individual and the date issued

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 following policies

- IT security and Acceptable Use Policy
- Social Media Policy
- Bring Your Own Device Policy
- Off-site working policy

and this accompanying guidance.

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 one of the school's HR Policies. 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 represent a 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/Headteacher.
- Staff should also act in accordance with the all the School's HR Policies and Child Protection/ Safeguarding policies.
- Staff should not access social media sites or leave these running in the background during working hours (contact time for teachers and teaching assistants), on any of the school's 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 photographs 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. Outline how such actions are likely to be damaging to the smooth running of the school and therefore the delivery to children.
- Respond quickly to those posting inappropriate comments. You may wish to issue a standard letter from the Chair of Governors asking them to contact the school/named person on a specific number. When following up, direct them to the appropriate processes for addressing issues or lodging complaints. Ensure the school's actions demonstrate both that harassment will not be tolerated and that expressing concerns through appropriate channels will ensure they are taken seriously.