ACCEPTABLE USE OF SOCIAL NETWORKING POLICY

This policy was reviewed in May 2017

This policy is due for review in May 2018.

1. Rationale

Connor Downs Academy is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation. Our own VLE has chat facilities and children are able to use this to talk to one another safely.

This policy and associated guidance is to protect staff, governor & pupils and to advise school leadership on how to deal with potential inappropriate use of social networking sites. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

2. Purpose

o To ensure that the school is not exposed to legal risk and liability

o To ensure that the reputation of the school is not adversely affected

o To give clear guidelines for staff, governors, pupils & other stakeholders on what they can and cannot say about the school.

o To help line managers to manage performance effectively.

o To help employees draw a line between their private and professional lives.

o To comply with the law on discrimination, data protection and protecting the health of employees.

o To set standards for good housekeeping - for example, for the use and storage of emails.

3. Scope

(ACAS advice & guidance on social networking)

This policy covers the use of social networking applications by all school stakeholders, including, employees, parents, governors and pupils. These groups are referred to collectively as 'school representatives' for brevity. The requirements of this policy apply to all uses of social networking applications which are used for any school related purpose and regardless of whether the school representatives are contributing in an official capacity to social networking applications provided by external organisations.

Acceptable behaviour and use of social networking applications includes, but is not limited to:

o Internet and emails

o Smart phones

o Blogs, for example Blogger

o Online discussion forums, such as netmums.com

o Collaborative spaces, such as Facebook

o Media sharing services, for example YouTube

o 'Micro-blogging' applications, for example Twitter

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Use of Social networking sites in work time

Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Head teacher.

Social Networking as part of school service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head teacher. However, school representatives must still operate in line with the requirements set out within the policy

School representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Connor Downs Academy expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

4. Terms of Use

Social Networking applications

o Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

o Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns in school hours or using the school name without permission from the Head of School.

o Must not be used in an abusive or hateful manner.

o Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.

o Must not breach the school's misconduct, equal opportunities or bullying and harassment policies.

o Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.

o No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with.

o Employees should not identify themselves as a representative of the school

o References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head of School.

o Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action. Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

5. Guidance/protection for staff on using social networking

o No member of staff should interact with any pupil in the school on social networking sites

o No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18

o This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.

o Where family and friends have pupils in school and there are legitimate family links, please inform the head teacher in writing. However, it would not be appropriate to network during the working day on school equipment

o It is illegal for an adult to network, giving their age and status as a child

o If you have any evidence of pupils or adults using social networking sites in the working day, please contact the Designated Child Protection Officer (Dan Kay) in school

6. Guidance/protection for pupils on using social networking

o No pupil under 13 should be accessing social networking sites when they are under the age required. This is the guidance from both Facebook and MSN. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is: http://www.facebook.com/help/contact.php?show_form=underage

o No pupil may access social networking sites during the school working day

o School computers are not to be used to access social networking sites at any time of day, other than our own E-Schools site

o Pupils are not allowed mobile phones in school except in exceptional circumstances where written permission has been given by the Head of School. All authorised mobile phones must be handed into the office at the beginning of the school day, the internet capability must be switched off. Failure to follow this guidance will result in a total ban for the pupil using a mobile phone

o No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens

o No school computers are to be used to access social networking sites at any time of day. o Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision

o Please report any improper contact or cyber bullying to your class teacher in confidence as soon as it happens.

o We have a zero tolerance to cyber bullying

7. Guidance/protection for parents on using social networking

Parents will be made aware of the school's policy on acceptable use of social networking sites by parents via the School Admissions Booklet, the annual beginning-of-year safeguarding newsletter and the school website. Where a parent or carer makes, shares or responds to any postings on social networking media that could be deemed as being defamatory of the school or individuals, bringing the reputation of the school into disrepute or placing a pupil or adult within the school community at risk of harm, the Head of School will contact those responsible for the postings inviting them to address any legitimate concerns about the school via the appropriate and established channels, e.g. the complaints procedure.

8. Child Protection guidance

If the head teacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they should:

o Record the disclosure in line with their Safeguarding & Child Protection policies

o Schools must refer the matter to the LADO who will investigate via MARU Team.

o If the disclosure has come from a parent, take normal steps to calm the parent and explain processes

o If disclosure comes from a member of staff, try to maintain confidentiality

o The LADO will advise whether the member of staff should be suspended pending

investigation after contact with the police. It is not recommended that action is taken until advice has been given.

o If disclosure is from a child, we follow our normal process in your child protection policy until the police investigation has been carried out

Cyber Bullying

By adopting the recommended no use of social networking sites on school premises, Connor Downs Academy protects itself from accusations of complicity in any cyber bullying through the provision of access. Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school. Incidences may occur of pupils posting concerning or inappropriate content on social networking sites out of school hours. A school is not obliged to take action over such content. However there might be circumstances in which wider concerns emerge from such circumstances. For example, those involved could be under the minimum age for participating in such activity or it might have taken place late at night in an unsupervised context. In such circumstance the school may wish to take advice from the local safeguarding team.

This can be a complex area, and these examples might help:

o A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.

o A child is receiving taunts from peers. It is all at weekends using MSN and Facebook. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.

o A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5: This is the tricky one. The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the schools recommendation. They could then deal with residual bullying in the school, but refuse to deal with the social networking issues.

Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted Anti Bullying Policy. If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment. This guidance can also apply to text and mobile phone cyber bullying.

9.Unpleasant and abusive postings

(Source: NAHT Social Networking Guidance document)

Where a school representative experiences untrue, inaccurate, abusive or defamatory postings relating to them being shared on social networking sites, the school will take appropriate action. The Head of School will contact those responsible for the postings inviting them to address any legitimate concerns about the school via the appropriate and established channels, e.g. the complaints procedure. Similarly where content is critical of the leadership and management of the school but not personally abusive, the Head of School or governors will contact and meet with those responsible for the postings. It may be appropriate for the Head of School and/or Chair of Governors to consider the matter in the same way as if the comments were made in a face-to-face context. Connor Downs Academy may decide to contact Legal Services department for guidance. There may be circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged.

If a school representative were to post an unprofessional, inaccurate, abusive or defamatory posting on a social networking site, the school will also take appropriate action which could result in disciplinary action. Staff may not make, share or respond to any postings on social networking media that could be deemed as:

- Being defamatory of the school or individuals
- Bringing the reputation of the school into disrepute
- Being in breach of their contract.
- Placing a pupil or adult within the school community at risk of harm.

10. NASUWT Social Networking - Guidelines for Members

Staff who are subjected to having unpleasant comments about them posted on sites are advised to take steps to have them removed. The procedure for different sites is provided below and has been derived from the 'teachtoday.eu website (with the exception of 'Twitter')

FACEBOOK: Facebook has changed its procedure since the previous guidance was published. There is now a 'report abuse' button on its pages. However, many members will not be account holders. In this circumstance you are advised to follow this link http://www.facebook.com/help/contact.php?show_form=report_tos_violation You can find Facebook's Statement of Rights and Responsibilities here.

MY SPACE Click on the 'Report Abuse' link at the bottom of every user profile page and other user-generated pages. To report inappropriate images, click on the image and select the 'Report this Image' option. MySpace also has a dedicated email helpline for school employees at schoolcare@myspace.com. You can find MySpace's Terms of Use here and MySpace's Guide for School Administrators here.

BEBO Click on the 'Report Abuse' link that is located below the user's profile photo (top left-hand corner of screen) on every Bebo profile page. In addition, you can report specific media content (eg photos, videos and widgets) to the Bebo customer services team by clicking on the 'Report Abuse' link located below the content you wish to report. You can find Bebo's Terms of Service here.

TWITTER The terms of service are not as clear as others regarding abusive comments. There is reference to 'specific threats of violence' and 'You may not use our service for any unlawful purposes' However, there are tight definitions of what constitutes violent threats. To further complicate matters. One needs to be a Twitter member to make a complaint.

YOU TUBE To report an inappropriate video on YouTube, you need to create a free account, log in, then click the 'Flag' link under the video. To report any abuse issues on the site, go to YouTube's Abuse and Policy Centre where you can choose from a number of options related to inappropriate content, abusive users, video takedowns and privacy issues. You can find YouTube's Community Guidelines here and its Terms of Use here.

LITTLEGOSSIP This is a relatively new site. Simply googling its name gives an indication of its

unsavoury nature. Badged as an opportunity to 'share the latest university and college gossip', the site has much school content. The newspapers have described it as an independent school problem but this is not accurate. Postings are anonymous and are generally malicious, spiteful and salacious and have the potential to cause considerable discord in schools. Members can find out if their school is involved by using the drop down box on the front page. There is evidence that schools will be taken down following contact with the site.

Facebook is targeted at older teenagers and adults. They have a no under 13 registration policy and recommend parental guidance for 13 to 16 year olds. The following are extracts from Facebook privacy policy: "If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us"

"We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices. Materials to help parents talk to their children about safe internet use can be found on this help page"

MSN recommend 13 but do not appear to have a policy of debarring younger pupils. There are many primary age pupils active on MSN

11. Privacy (NASUWT Social Networking - Guidelines for Members)

Sites such as Facebook (minimum age requirement is 13 years) and Twitter (services are not directed to persons under 13 years) can serve as a learning tool where training videos and other materials are made easily accessible to students in a user-friendly and engaging way. However, the open nature of the Internet means that social networking sites can leave professionals such as teachers vulnerable if they fail to observe a few simple precautions. The below guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position.

To ensure that a Facebook account does not compromise a member of staff's professional position, staff should ensure that their privacy settings are set correctly.

Staff should not under any circumstances accept friend requests from a person they believe to be either a parent or a pupil at your school. As a minimum, the following is recommended

Privacy Setting Recommended security level Send your messages Friends only See your friend list Friends only See your education and work Friends only See your current city and hometown Friends only See your likes, activities and other connections Friends only Your status, photos, and posts Friends only Bio and favourite quotations Friends only Family and relationships Friends only Photos and videos you're tagged in Friends only Religious and political views Friends only Birthday Friends only Permission to comment on your posts Friends only Places you check in to Friends only Contact information Friends only

Staff should always make sure that they log out of Facebook after using it. Any account can be hijacked by others if a member of staff remains logged in – even if they quit their browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Staff should make sure they clear their chat history on Facebook (click "Clear Chat history" in the chat window).

Staff should be aware that employers may scour websites looking for information before a job interview. Staff should take care to remove any content that they would not want them to see.

12. Stakeholder/Staff conduct on social networking sites

(NASUWT Social Networking - Guidelines for Members)

Staff should act in accordance with the school's ICT policy and any specific guidance on the use of social networking sites.

Staff should always be mindful that other users could post a photo on their profile in which a member of staff is named, so staff need to be remain aware & responsible regarding any photos they may appear in. On Facebook, staff can 'untag' themselves from a photo. If they do find inappropriate references to themselves and/or images of themselves posted by a 'friend' online they should contact them and the site to have the material removed.

Staff need to be aware that parents and students could potentially access a member of staff's profile and could, if they find the information and/or images it contains offensive, report this immediately to their employer.

If staff have any concerns about information on their social networking site or if they feel they are the victim of cyberbullying, they should inform their employer and may also wish to contact

their union too.

Staff should not publish their date of birth or home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to bank or credit card accounts.

Staff should be aware that routine monitoring of the school's network is carried out by our ICT support contractor as part of our annual service contract.

Staff should prevent their network provider from passing on their details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click "Privacy Settings". Under "Applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.

Staff should ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

Staff should not make disparaging remarks about the school. They should be aware that doing this in the presence of others may be deemed as bullying and/or harassment.

13. Monitoring & Evaluation

Acceptable use of social networking is always a matter of concern to all of our hub governors.

Date of adoption: May 2017 Date of review: May 2018