Title	**Social Networking Policy**
Document Type	Approved
Author	Data Protection Enterprise Ltd
Owner	Headteacher
Subject	Social Networking
Government Security Classification	Official
Document Version	Version 1
Created	01/02/2022
Approved by	Board of Governors
Review Date	31/03/2023 or earlier where there is a change in the applicable law affecting this Policy Guidance

Equality Impact Assessment

The school aims to design and implement services, policies and procedures that meet the diverse needs of our provision, population and workforce, ensuring that none are placed at an unreasonable or unfair disadvantage over others. We are confident that this policy does not place anyone at an unreasonable or unfair disadvantage, and is compliant with relevant equalities legislation.

Where the school or staff are referred to, the policy and the following procedures apply to all staff working for Corbets Tey School on all sites.

Version Control

Version	Date	Author	Description of Change
1	20/01/2022	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	New Policy

Contents:

1. INTRODUCTION

Social networking sites such as Facebook and Twitter are now widely used. This type of media allows people to communicate in ways that were not previously possible that can positively enhance means of communication. The School is aware and acknowledges that increasing numbers of adults and young persons are using social networking sites. The widespread availability and use of social networking applications 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.

This policy and associated guidance are to protect staff and advise school leadership on how to deal with potential inappropriate use of social networking sites. For example, our use of social networking application has implications for our duty to safeguard students, young people and vulnerable adults.

Social networking applications include but are not limited to:

- Blogs i.e. blogger;
- Online discussion forums, for example Facebook, Snapchat, Instagram
- Media sharing services for example YouTube;
- 'Micro-blogging' application for example Twitter;
- 'DM's' (direct messages) within applications such as Instagram or Facebook

2. OBJECTIVES

The purpose of this policy is to ensure:-

- That the School is not exposed to legal and governance risks;
- That the reputation of the School is not adversely affected;
- That our users are able to clearly distinguish where information has been provided via social networking applications, that it is legitimately representative of the School;
- Protocols to be applied where employees are contributing in an official capacity to social networking applications provided by external organisations;
- Safeguarding of students, staff and anyone associated with the School from the negative effects of social networking sites;
- What the school considers to be appropriate and inappropriate use of social networking by staff;
- the reputation of the School, other schools, other organisations and employers from unwarranted abuse through social networking; and
- Set out the procedures that will be followed where it is considered that staff have inappropriately or unlawfully used social networking.

3. SCOPE

This policy covers the use of social networking applications by all school stakeholders, including employees, governors and students. These groups are referred to 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 a personal capacity or an official capacity to social networking applications.

4. RESPONSIBILITY AND ACCOUNTABILITY

Headteachers:

- Should ensure that all existing and new staff are trained and become familiar with this policy and its relationship to the School's standards, policies and guidance on the use of ICT and online safety;
- Should provide opportunities to discuss appropriate social networking use by staff on a regular basis and ensure that any queries raised are resolved swiftly;
- Must ensure that any allegations raised in respect of access to social networking sites are investigated promptly and appropriately, in accordance with the School's disciplinary procedure, code of conducts and internet safety guidelines; and
- Should ensure there is a system in place for regular monitoring

School Staff

- Should ensure that they are familiar with the contents of this policy and its relationship to the School's standards, policies and guidance on the use of ICT and online safety;
- Should raise any queries or areas of concern they have relating to the use of social networking sites and interpretation of this policy – with their line manager in the first instances; and
- Must comply with this policy where specific activities or conduct is prohibited.

School Governors

- Will review this policy and its applications when a review is required (or more frequently as maybe necessary); and
- Should ensure that their own behaviour is in line with that expected

5. ACCESS TO SOCIAL NETWORKING SITES

There is an official YouTube channel and a school Twitter account maintained by the School Enterprise and Technology Lead. This might include internal forums for staff and outward facing forums for school activities/clubs etc.

Restricted access for 'official' work purposes is permitted for the above-named applications, where explicit permission has been given by the Headteacher.

The use of social networking applications in work time for personal use is not permitted.

6. SCHOOL MANAGING SOCIAL NETWORKING SITES ('OFFICAL USE')

It is important to ensure that employees, members of the public and other users of online services know when a social networking application is being used for official School purposes.

To assist with this, all employees must adhere to the following requirements:

- 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 Headteacher first.
- Only use an official (i.e. not personal) email address or account name which will be used for official purposes. Staff must not use "personal" accounts to comment on "official" school business.
- The School's logo and other branding elements should be used where appropriate to indicate the school's support. The School's logo should not be used on social networking applications which are unrelated to or are not representative of the School's official position.

- Employees should identify themselves as their official position held within the School on social networking applications' e.g. through providing additional information on user profiles.
- Employees should ensure that any contributions on any social networking application they make are strictly professional, remain confidential, uphold the ethos and reputation of the School and do not give rise to bringing the school into disrepute.
- Staff should not spend an unreasonable or disproportionate amount of time during the working day developing and maintaining or using sites.
- Employees must not promote or comment on personal, political, religious or other matters.
- Pictures of young person's taken should follow the guidance set out within the schools Acceptable Use Policy.
- Employees should be aware that sites will be monitored.
- The Enterprise and Technology Lead will approve "friendship"/" follow" requests from parents within School-authorised Twitter and YouTube account/s, but not students.
- Staff must follow statutory and school safeguarding procedures at all times when using social media and must report all situations where any young person is at potential risk by using relevant statutory and school procedures
- Staff must not use school social media for any personal discussions or for any individual personal matters even if initiated by other members of the school community. Users must be directed to more appropriate communication channels.
- Staff must ensure that all social media use when working with students is sanctioned by the school; only uses explicitly agreed social media; and follows agreed policies and procedures

7. PERSONAL SOCIAL NETWORKING SITES

All employees of the School 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 and the Safeguarding Vulnerable Groups Act 2006.

Any communications of content published on a social networking site which is open to the public view, may be seen by members of the school community. Employees hold positions of responsibility and are viewed as such in the public domain. Inappropriate usage of social networking sites by employees can have a major impact on the employment relationship. Any posting that causes damage to the school, any of its employees or any third party's reputation may amount to an investigation under the School Disciplinary Procedures, which could result in gross misconduct and potentially, dismissal.

When contributing to personal posts, staff should be mindful of the audience, not disclose sensitive or confidential information about the School and not risk bringing the School into disrepute.

Employees should not use personal sites for any professional activity. The School reserves the right to require the closure of any applications or removal of content published by employees which may adversely affect the reputation of the school or put it at risk of legal action.

Anyone who becomes aware of inappropriate postings on social networking sites, must report it to their line manager as soon as possible. The line manager will then follow the disciplinary procedure. If an employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate and falls within the remit of this policy, then that employee may be subject to disciplinary procedure.

i. Posting inappropriate images

Incident images of any employee that can be accessed by students, parents or members of the public are unacceptable and can lead to young person protection issues as well as

bringing the School into disrepute. Staff must not post pictures of school students within personal sites.

ii. Posting inappropriate comments

It is unacceptable for any employee to discuss students, parents, work colleagues or any other member of the school community on any type of social networking site. Reports about oneself may also impact on the employment relationship for example, if an employee is off sick but makes comments on a site to the contrary.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. The School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration of the rights of others and strictly in accordance with other related school policies.

iii. Social interaction with students (past and present)

Employees should not interact with or engage in conversation whatsoever with any young person under the age of 18 that they come into contact within their professional capacity on any personal social networking site. This may include for example, students and their siblings or students on placement or work experience, past or present. Offers of assistance to a student with their studies via any social networking site are inappropriate and also leaves the employee vulnerable to allegations being made. Should an employee become aware of an underage person using social networking sites, (Facebook and WhatsApp for example, have this set at 13 years), they should report this to the Headteacher.

iv. Making friends

Employees should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. We recommend that school staff ensure that personal social networking sites are set at “private”. We also strongly advise that school staff are mindful of the potential audience when posting comments and sharing information/posts.

Whilst we acknowledge that it might not be always possible to do so in a context where staff live local to a school community, we recommend not listing parents as approved contacts.

Being mindful of this guidance will reduce the risk of employees being vulnerable to allegations being made.

v. We advise that personal social networking application should not:

- Be used to publish any content which may result in actions for breach of contract, defamation, discriminations, breaches of copyright, data protection, breach of confidentiality, intellectual property rights or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature including any radicalised, terrorist or extremist political or religious viewpoint that may bring the School into disrepute. Some examples are given in Appendix A;
- Be used for party political purposes of specific campaigning purposes as the School is not permitted to publish any material which ‘in whole or part appears to affect public support for a political party’ (LGA 1986);
- Be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- Be used in an abusive or hateful manner;
- Be used for actions that would put other employees in breach of the Code of Conduct Policy;

- Be in breach of the school's disciplinary and equal opportunities policies;
- Be used to discuss or advise any matters relating to school matters, staff, students or parents

vi. Additional responsibilities governing the personal use of social networking applications

- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, student, parent or school activity/event.
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the School or detrimentally effects the School's reputation then the School is entitled to take disciplinary action.
- It is illegal for an adult to network online, giving their age and status as a young person.
- Anyone with evidence of students or adults using social networking sites in the working day, should contact the named Child Protection Lead in school.

Where individuals from partner organisations are involved and are acting on behalf of the School they will also be expected to comply with the relevant policies.

8. GENERAL GUIDANCE/PROTECTION FOR STUDENTS/VISITORS/OLDER STUDENTS ON USING SOCIAL NETWORKING SITES

- No student under 13 should be accessing social networking sites. There is a mechanism on Facebook where students can be reported via the Help screen.
- No student may access social networking sites at School at any time of day.
- No student should attempt to join a staff member's areas on networking sites. If students attempt to do this, the member of staff is to information the Headteacher. Parents will be informed if this happens.
- Please report any improper contact or cyber bullying in confidence as soon as it happens/ we have zero tolerance to cyber bullying

9. CYBER BULLYING

- The signs and effects of Cyber Bullying will be taught during ICT and PSHE lessons and within assemblies, including how to whistle blow this to an adult. By adopting the recommended 'no use of social networking sites' on school premises, the School protects themselves from accusations of complicity in any cyber bullying through the provision of access.
- Parents should be aware of the Schools policy of access to social networking sites.
- Where disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the School.

10. LINKS WITH OTHER POLICIES

This Social Networking Policy is linked to the School:

- Data Protection Policy
- Freedom of Information Policy
- Security Incident and Data Breach Policy
- Acceptable Use Policy
- Safeguarding Policy

The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk

Appendix A – Examples of unacceptable behaviour using Social Networking Sites

1. **Breach of Contract**

   There is an implied term of mutual trust and confidence between the School (employer) and employee in all employment contracts. A very negative and damaging posting or communication on a social networking site about the School or colleagues may entitle the Headteacher/Line Manager to decide that this term has been broken. Such conduct would be subject to the School's disciplinary procedure.

2. **Defamation**

   If an employee places defamatory information or material on a social networking site such as bad mouthing another colleague or a student of the School, such conduct would be subject to the School's disciplinary procedure and could lead to the employee's dismissal

3. **Discrimination**

   The School's recruitment and selection policy provide the correct and proper procedures to be used in the recruitment and selection of staff. Candidates should be selected on the basis of testable evidence provided on application forms and through the selection process and references as provided by the applicant. Under no circumstances should information from the social networking sites be used to make selection decisions. Such action could result in expensive discrimination claims. For example – not all candidates will have profiles on social networking sites and using information from this source may be seen as giving an unfair advantage or disadvantage to certain candidates, possibly discriminating against younger people who are likely to use social networking sites more often.

   Many forms of discrimination claims, including harassment claims can occur via emails, if an employee places discriminatory material about another employee, a member of the Governing Body, parents, students, young people and vulnerable adults, this could amount to bullying or harassment of that individual. The School may be vicariously liable for such acts unless it took such steps that were reasonably practicable to prevent material being place on a site. Where an employee carries out an act of harassment or discrimination in the course of their employment, the School is vicariously liable for that act even when the act is unauthorised. Once an issue of email harassment has been raised and the harasser identified, immediate action should be taken to stop the harassment and instigate the disciplinary procedure whilst supporting the harassed employee.

4. **Breach of Health and Safety**

   For example, an internet video clip of employees performing stunts wearing the organisation's uniform. When information like this is found, the School should follow the School's disciplinary procedure to investigate the possibility of a breach of health and safety legislation on the part of the employee. If the School is aware of this and fails to investigate there may be liability for personal injuries in the law of negligence.