Social Media Policy

The organization recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Purpose of the policy:

- The purpose of this policy is to encourage good practice, to protect the organization and its employees, and to promote the effective use of social media as part of the organization activities.
- This policy covers personal and professional use of social media and aims to encourage its safe use by the organization and its employees.
- The policy applies regardless of whether the social media is accessed using the IT facilities and equipment, or equipment belonging to members of staff.
- Personal communications via social media accounts that are likely to have a negative impact on professional standards or the organization's reputation are within the scope of this policy.
- This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers.

Roles, responsibilities and procedure:

Employees should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensure that any use of social media is carried out in line with this policy;
- be aware that any excessive use of social media in the organization may result in disciplinary action;
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees of the organization, or even future employers, to read. If in doubt, don't post it!

Managers are responsible for:

- addressing any concerns and/or questions employees may have on the use of social media;
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.

Human Resources (HR) is responsible for:

- giving specialist advice on the use of social media;
- implementing and reviewing this policy.

Definition of social media:

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, and YouTube.

Acceptable use:

Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

Employees should not upload any content on to social media sites that:

- is confidential to the organization or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the organization into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the organization and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the organization's social media accounts. Employees should note that the use of social media accounts during lesson time is not permitted.

Safeguarding:

The use of social networking sites introduces a range of potential safeguarding risks to children and young people.

Potential risks can include, but are not limited to:

- online bullying;
- grooming, exploitation or stalking;
- exposure to inappropriate material or hateful language;
- encouraging violent behaviour, self-harm or risk taking.

In order to mitigate these risks, there are steps you can take to promote safety online:

- You should not use any information in an attempt to locate or meet a child.
- Ensure that any messages, photos or information comply with existing policies.

Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the higher authorities of the organization.
- Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.
- With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

Reporting, responding and recording cyberbullying incidents:

- Staff should never engage with cyberbullying incidents. If in the course of your employment with this organization, you discover a website containing inaccurate, inappropriate or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager in the organization.
- Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

Action by employer: inappropriate use of social media:

- Following a report of inappropriate use of social media, the senior manager will conduct a prompt investigation.
- If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the organization's behaviour policy.
- The senior manager, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, i.e., within 24 hours. If the website requires the individual who is complaining to do so personally, the organization will give their full support and assistance.
- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website.
- If the material is threatening and/or intimidating, senior management will, with the member of staff's consent, report the matter to the police.
- The member of staff will be offered full support and appropriate stress counselling.

Breaches of this policy:

Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the organization's bullying or disciplinary procedure. The member of staff will be expected to co-operate with the organization's investigation which may involve:

- handing over relevant passwords and login details;
- printing a copy or obtaining a screenshot of the alleged unacceptable content;
- determining that the responsibility or source of the content was in fact the member of staff.

The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the organization or the individuals concerned. Staff should be aware that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee. Where conduct is considered to be unlawful, the organization will report the matter to the police and other external agencies.

Monitoring and review:

If the manager reasonably believes that an employee has breached this policy, from time to time the will monitor or record communications that are sent or received from within the organization's network.

This policy will be reviewed on a yearly basis and, in accordance with the following, on an as-and-when-required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported.

This policy does not form part of any employee's contract of employment and may also, be amended from time to time by the organization.