

Herons' Moor Academy



E-Safety Policy

Reviewed by	Rosie Vian	June 2018
Approved by	Education Quality Committee	17 th June 2019
Endorsed by	Full Governors	July 4 th 2019
Next Reviewed:	June 2020	

E-SAFETY POLICY

Rationale

The purpose of this policy is

- To provide all staff and volunteers working at Herons' Moor with guidance on how the internet is to be used within the Academy.
- To ensure staff use social networking sites safely and securely.
- To ensure that staff are aware of their responsibilities in connection with the use of social networking sites and of the risks associated with the inappropriate use of social networking sites and any impacts in relation to their employment
- To ensure that staff are aware of the risks associated with inappropriate use of social networking sites, how to minimise the risk that they make themselves vulnerable to allegations and how these may impact on their employment.
- To ensure the Governing Body maintains its duty to safeguard children, the reputation of the Academy, the IFT and the wider community

This policy should be read in conjunction with the Academy Code of Conduct which comprises 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' and Part 1 of "keeping children safe in education".

In this Policy colleague' means all individuals engaged by the Academy or in the Trust in a paid or voluntary capacity including parent helpers and governors, those on work experience placements and agency colleagues. Third parties acting on behalf of or in partnership with the school are also expected to adhere to this guidance.

Staff are not discouraged from using social networking sites. However, all staff, volunteers and placement students should be aware that the Governing Body will regard any occasions where the services are used inappropriately as serious misconduct . Instances of on-line or cyber bullying and harassment will be regarded as a serious matter and will be dealt with under the Academy's Disciplinary Policy. Any Academy colleague who is being bullied or harassed on-line or is the subject of inappropriate messages or false allegations should report this to the Headteacher and/or the Local Governing Board.

In the event that this Policy is not followed or any instances of the inappropriate use of social networking sites are brought to the attention of the Academy, these may be investigated under the Academy's Disciplinary Policy and depending on the seriousness of the matter disciplinary action may be taken which may result in dismissal. A serious breach of the Policy may be regarded as gross misconduct, leading to summary dismissal.

Where any allegations have a children's safeguarding dimension (that is, where an individual has:

- behaved in a way that has harmed a child, or may have harmed a child;
- possibly committed a criminal offence against or related to a child or

- behaved towards a child or children in a way that indicates he or she would pose a risk of harm to children)

The Local Authority Designated Officer (DOFO) must be contacted via the Social Care's Single Point of Access on 01275 888808 at the earliest opportunity and the Allegations of Abuse procedure outlined within the DfE's *Keeping Children Safe in Education* guidance must be followed (this is available on the NSESP website or on the DfE website at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447595/KCSIE_July_2015.pdf .

Guidelines

General Internet Usage

Adults are not permitted to visit websites that contain or relate to:

- pornography
- discrimination of any kind
- racial or religious hatred
- illegal acts
- any other information which may be offensive to colleagues or deemed inappropriate

No posts, downloads, uploads, remarks, or comments should be made on such websites.

On occasions where accessing such sites may be deemed appropriate for curricular reasons, for example to address racial issues, activities must be pre-planned and submitted to the Headteacher so that evidence is kept in case of an investigation.

Any incident when a member of staff is deemed to have deliberately accessed sites containing images of child abuse, adult material that breaches the Obscene Publications Act in the UK or criminally racist material will be considered gross misconduct and will result in a report being filed to the police.

Staff should not use the Academy internet connection

- To run a business.
- For personal financial or domestic business unless completely unavoidable.
- To upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties (e.g. music downloads, copyrighted pictures etc.).
- To reveal or publicise confidential or proprietary information, including sensitive data relating to children or other staff members.
- To send or receive large files, or large numbers of small files, that would seriously hinder other's uses of the internet.
- To solicit, represent personal opinions or revealing confidential information.

Personal devices such as tablets, mobile phones and personal laptops are not to be used to access the Academy's wireless network.

Mobile phones and other such devices are only to be used in 'staff only' areas i.e., staff room, offices etc.. **Please also refer to the appropriate use of electronic communication within the Campus Policy on the Use of Mobile Phones.**

Usage of the internet is monitored via the SWGfL and any inappropriate usage is communicated to the Academy.

Any images (still or moving) of children are to be recorded using Academy equipment only and should be stored securely and not taken off the premises.

In the event that the above guidelines are breached accidentally, staff are required to make a report to the E-Safety leader or Headteacher who will, if appropriate, notify the SWGfL for monitoring purposes.

REPLACE WITH:

Social Networking

- 1. Colleagues at the academy must not access social networking sites for personal use via school information systems or using school equipment;**
- 2. Colleagues at the academy must not accept pupils as friends or use internet or web-based communication channels to send any personal messages to pupils directly or indirectly (for example via the parents of pupils) – personal communication could be considered inappropriate and unprofessional and makes colleagues at the academy vulnerable to allegations;**
- 3. Colleagues at the academy are strongly advised not to be friends (on or off line) with recent pupils (the potential for colleagues at the academy to be compromised in terms of content and open to accusations makes the risk not worth taking) and colleagues at the academy are also strongly advised not to be friends with pupils at other academies or schools (on or off line) as this is likely to make them vulnerable to allegations and may be open to investigation by the Local Authority or police. Where a colleague is considering not following this advice, they are required to discuss the matter, and the implications with the Headteacher or designated safeguarding lead.**
- 4. Any pupil-initiated communication, on-line friendships/friend requests must be declined and reported to the Headteacher or designated safeguarding lead (If a colleague receives messages on his/her social networking profile that they think could be from a pupil they must report it to their line manager/Headteacher and discuss whether it is appropriate for the colleague to contact the internet service or social networking provider so that the provider can investigate and take the appropriate action);**

5. Colleagues at the academy must not share any personal information with any pupil (including personal contact details, personal website addresses/social networking site details);
6. Colleagues at the academy must not place/post any material (or links to any material) of a compromising nature (that is, any material a reasonable person might find obscene or offensive (such as sexually explicit or unlawfully discriminatory material) including inappropriate photographs or indecent remarks or material relating to illegal activity) on any social network space;
7. Colleagues at the academy are advised not to write about their work but where a colleague at the academy chooses to do so:
 - he/she must make it clear that the views expressed are his/hers only and do not reflect the views of the academy/IFT (and all other guidelines in this policy must still be adhered to when making any reference to the workplace)
 - he/she must not discuss pupils, colleagues, parents or carers and
 - he/she must not disclose any information that is confidential to the academy or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act or disclose any information about the academy/IFT that is not yet in the public arena;
8. Colleagues at the academy must not post or share photographs of pupils under any circumstances and must not post or share photographs of colleagues or parents without their express permission;
9. Colleagues at the academy must not make what could reasonably be perceived as abusive/defamatory/undermining/derogatory/critical remarks about the academy/colleagues/pupils/parents/governors or the IFT or post anything that misrepresents or could potentially bring the academy/IFT into disrepute;
10. Colleagues at the academy must not disclose confidential information relating to their employment at the academy;
11. Colleagues at the academy must not link their own sites to the academy website or use the academy's or the IFT's logo or any other identifiers on their personal web pages;
12. If any colleague at the academy receives media contact regarding the content of their site or is offered payment for site content which relates to the academy they must consult their Headteacher/line manager;
13. Colleagues at the academy must not use any internet/on-line resources to seek information on any pupil, parent or other colleague at the academy other than for the purposes of legitimate monitoring of the usage of Social Networking sites by designated managers / officers.
14. Colleagues at the academy must not use social networking sites to seek to influence pupils regarding their own political or religious views or recruit them to an organisation of this kind using their status as a trusted adult to encourage this
15. All colleagues must make themselves aware of and act in accordance with their duties under the DfE statutory guidance *Keeping Children Safe* as these relate to:
 - their own on-line activity

- the on-line activity of pupils and other colleagues and
- information of which they become aware on-line

including their duties relating to Children Missing from Education, Child Sexual Exploitation, FGM and Preventing Radicalisation (Prevent).

All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended (social networking sites are public forums). Colleagues at the academy are strongly advised, in their own interests, to take steps to ensure as far as possible that their on-line personal data is not accessible to anybody who they do not want to have permission to access it. For example, they are strongly advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum and, where relevant, use strong passwords and change them regularly.

Conclusion

While the internet is a valuable teaching resource, it is important that it is used correctly and legally, and it is the duty of all members of staff to set an example of acceptable and safe internet usage for the children at our Academy. Staff should never behave in a manner which could leave them vulnerable to accusations of misconduct.

The academy reserves the right to take action to obtain the removal of any content posted by colleagues at the academy which may adversely affect the reputation of the academy (or any colleague, governor, pupil or parent at the academy) or put it at risk of legal action. Should the academy decide to pursue this course of action, the advice of the IFT/Weston College Marketing and Communications Team may be sought.

RELEVANT POLICIES / GUIDANCE

- Keeping Children Safe in Education (DfE statutory guidance)
- Guidance for Safer Working Practice (formerly DfE guidance, revised by the Safer Recruitment Consortium in 2015)
- Disciplinary Policy and Procedure
- Code of conduct
- Equality Scheme / Policy
- ICT Policy/Acceptable use Policy
- E-Safety Policy
- Whistleblowing Policy

LEGISLATION

The following legislation must be considered when adhering to this policy:

- Obscene Publications Act 1959

- Protection of Children Act 1988
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Defamation Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010

Reviewed by Finance Cttee 14 th Oct. 10. Endorsed by FGB 25 th Nov. 10	Reviewed by Staffing Cttee. 22 nd April 2013. Endorsed by FGB 13 th May 13	Reviewed by Staffing and Curriculum Cttee 28 th April 2014. Endorsed by FGB 12 th May 2014	Reviewed by Staffing and Curriculum Cttee 27 th April 15. Endorsed by FGB 11 th May 15.	Reviewed by Staffing and Curriculum Cttee 23 rd April 16. Endorsed by FGB 9 th May 16.	Reviewed by Staffing and Curriculum Cttee 12 th June 2017 Endorsed by FGB July 2017	Reviewed by Ed Quality Cttee 11 th June 2018 Endorsed by FGB June 2018
---	---	---	--	---	---	--