STAFF PROFESSIONAL IDENTITY PROTECTION POLICY

Reviewed and updated: March 2022
Next review: March 2025
Status: non-statutory

This policy should be read with reference to the following policies:

- Internal data security policy.
- ICT and use of the internet and intranet by staff.
- Social media.
- E-safety
- Staff email.
- Use of personally owned devices by staff (BYOD).

Background

The need for everyone to use electronic communications grows apace. School staff need guidance on how to employ tactics to protect themselves from potential harassment when using electronic communications, and on how to protect the identity and image of the school by which they are employed.

What is an online reputation?
An online reputation is the perception, estimation and opinion that is formed when an individual is encountered online. This could be when someone:

- Visits a social networking profile.
- Reads a comment about an individual posted on another profile.
- Sees online photo albums or images with the individual in them.

Indeed, any instance or reference which either the individual has posted, or someone else has posted, builds up the digital footprint of a person.

An online reputation will be formed through:

- Posts by an individual.
- Posts by others but about an individual or linked to the individual.
- Posts by others pretending to be the individual.

Who does it affect?
Everyone! Obviously it applies to those who post online. However, because other people could be posting information, a person does not even have to have been on the internet before to have an

online reputation! A survey conducted by AVG concluded that 23% of unborn children already have a digital footprint.

Why is online reputation important to any individual?

- Your reputation should be important to you because it is a tool that others could and will use to make decisions about you. Clearly this could have a dramatic effect on your personal and professional lives, especially if your digital footprint is poor.

- What does your profile picture or avatar (the image by which you represent yourself) say about you?

How is your online reputation different?

- Remember that the internet never forgets – when you post something online it will always be there.

STAFF PROFESSIONAL IDENTITY PROTECTION POLICY

Introduction

Electronic communications equipment includes (but may not be limited to):

- Telephones, faxes, voice-mail, computers, laptops, internet, mobile phones (all types), photocopiers, digital cameras, walkie-talkies, web cameras, videos and palm-held equipment.

Types of communication can include (but may not be limited to):

- Telephone calls, email, text messaging, multimedia messaging, transmission of photographs and moving pictures, contact via websites and social network sites, blogging, wikis, contact via web cameras and internet phones.

Members of staff need to protect themselves from potential harassment when using electronic communications. It is also essential that Elthorne Park High school's reputation is not damaged by ill-considered use of electronic communications by staff, who might face consequential disciplinary action as a result.

Objectives and targets

This policy aims to provide information and guidance to protect school staff from harassment, real or alleged, misuse, and any consequential disciplinary action arising from the use of electronic communication equipment in or outside school. It is also intended to ensure that the school's equipment is used responsibly and safely at all times, because if school systems are not used responsibly, and in line with this policy and advice, there could be major implications for both individuals and the school as a whole.

Action plan

Staff are advised to pay close attention to the misuses listed below and throughout this staff professional identity protection policy because this document is produced for your protection.

Professional identity protection – overview for staff

- In communications with pupils and parents, **never** give out personal information which identifies your:
    - Home address.
    - Telephone number.
    - Personal mobile phone number.
    - Personal email address.

Once such information is known, you are open to harassment through unwanted phone calls, text messages and emails.

- Avoid the use of chat rooms, instant messaging or other social networking services which are accessed socially by pupils and are not monitored by the school.

- Ensure you do not:
  - Accept pupils and/or parents as ‘friends’ on your personal social network site.
  - Use your school email address as contact on any social networking sites.
  - Add photos from school events, trips or photos of pupils.
  - Add the name of where you work.
  - Join associated groups.
- Protect your social network site by using the **correct up-to-date** privacy settings.
- Make sure that personal information **cannot** be seen from the links to your friends’ sites.
- Make up your ‘friend groups’ to limit the people you share information with.
- Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Log off, turn it off and set up a password-protected screen saver to prevent unauthorised access.
- Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login detail because you will then be held responsible for their online activity.
- Always use the school’s digital camera or video camera for taking pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera’s memory. Photographs of children should not be taken home to use on a personal computer.
- Always speak professionally and respect confidentiality and be aware that the message could be overheard at either end when using any hand-held school walkie-talkies.
- If you are using school electronic equipment off-site, then take the same level of care as you would in school. A digital camera taken off-site should not be returned to school with personal photographs on it.
- Do not make personal financial transactions on any school equipment because information may become accessible to others.
- Observe sensible precautions when taking photographs which may include pupils. Make sure that individual pupils cannot be identified by name, especially if the photograph is for use on the school website or virtual learning environment (VLE).
- Report immediately, and in writing, to the designated person/headteacher, any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep hard copies and e-copies as evidence. (Refer to school policies for further guidance on this issue.)

Professional identity protection – the school's responsibility
The school will:

- Enforce policies to protect staff and pupils from malicious use of mobile phones, in particular the use of camera- and video-phones.
- Ensure that the policy and procedures for home-school communication are shared with, and understood by, all staff.
- Establish whole school systems for dealing with inappropriate messages and breaches of security.
- Provide all staff with a personal email address to be used for all school-related communications by every member of staff.
- Establish a clear school policy for monitoring the use of the school's electronic equipment by staff, including procedures for accessing email and files when staff are absent due to holiday, illness, etc.
- Provide digital cameras and mobile phones which can be borrowed by staff as required for all school-related work, including trips. These mobile phone numbers should be used on the emergency parental telephone trees for trips.
- Provide a safe learning environment, such as a VLE, for electronic communications with pupils.
- Ensure there are established systems for reporting unwanted or accidental electronic communications and that all staff are aware of the correct person to report any issues to.
- Ensure all incidents reported are correctly recorded and that such incidents are always treated seriously.
- Create procedures to regularly check the school's presence on the web to ensure material detrimental to the school is not published.
- Ensure all staff are trained regularly on safeguarding matters, including online safety.

Email
Please refer to the separate staff email policy which covers:

- Managing emails.
- Sending emails.
- Receiving emails.
- Emailing personal, sensitive, confidential or classified information.

And remember:

- All school business should be carried out using your work email address.

- Never give a personal email address to pupils/parents.

- It is impossible to control what information is sent to a member of staff by email. However, if offensive, obscene and/or discriminatory material is received, the recipient must report it immediately, and in writing, to the designated person in school (or the headteacher). Never send a reply. Keep a printed copy of the email as evidence and pass a copy of the email to the appropriate person (complaints officer) for the record. Ensure that the sender's information is also recorded because their email service provider may take action.

Social networks, blogs and wikis
Many staff and virtually all pupils use a computer for social activities outside school. Staff should take careful note of the following:

- Staff should not use school facilities to access or update their personal social networks.

- Staff should be aware of the potential risk to their professional reputation of adding pupils, parents or friends of pupils as 'friends' on their social network site and are strongly recommended not to do so.

- Comments made on a social network site or weblog (blog) which relate to the school or pupils in the school have the potential to be misinterpreted and could result in disciplinary action.

- Photographs and descriptions of activities in the personal life of staff may also not be considered appropriate if viewed by other staff, pupils or parents.

- Staff should be aware that, even if they have used the privacy settings, they may not be able to prevent material becoming public from their 'friends' sites.

- It is recognised that these online communications tools, such as blogs and wikis, have a potentially useful role in schools – such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families are sharing these tools with staff in school it is important that this should always be through a school-based provision, such as the school learning platform/VLE, using a school log-in where all communication is open and transparent.

- If staff keep a personal blog, the content must always maintain acceptable professional standards because any inappropriate use may lead to disciplinary action in accordance with school policy.

- All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school.

Action you must take if you discover inappropriate (threatening or malicious) material online concerning yourself or your school
Both the school and members of staff are vulnerable to material being posted about them online. All staff should be aware of the need to report this should they become aware of anything bringing the school or colleagues into disrepute.

- Secure and preserve any evidence. For example, note the web address (URL) or take a screen shot or copy and print the screen.

- Report it immediately to your line manager or headteacher.

- All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others. If the material has been created by a pupil or parent, then the school has a responsibility to deal with it. The school will contact the uploader of the material or the internet service provider/site administrator and ask for the material to be removed.

Real time online communication
This refers to using web cameras, chat (MSN), skype, facetime, mobile phone etc.

The ability to communicate in real time using the computer and other electronic devices (such as mobile phones) makes these an excellent tool for a range of educational purposes. However, staff should take the same level of care with these tools as they would if working in a face-to-face situation with a pupil or group of pupils.

- Access should always be through a school created account, never a personal account, and it should be focused on a clearly specified educational objective.

- There are likely to be times when this kind of activity will happen outside normal school hours and perhaps off the school premises e.g. visits, fixtures, field trips etc. In this situation, it should always be carried out with the full knowledge and agreement of your line manager or headteacher.

- Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social occasion.

- When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge. However, they may wish to use this function for their own security, as long as all parties are informed that recording is taking place.

- Staff must protect their privacy by never allowing pupils or parents to obtain their mobile phone number or leave their mobile phone where it could be accessed by a pupil.

*Action staff **must** take if an incident occurs:*
- Report immediately, and in writing, to your line manager or headteacher.

- Do not reply to abusive or worrying text or video messages.

- Do not delete messages. Keep them for evidence.

- Use 1471 to try and obtain the number if you can. Most calls can be traced.

- Report it to your phone provider and/or request a change of number.

- Technical staff may also be able to help you to find or preserve evidence eg logs of the call.

Employees must not use school equipment (including their school provided laptop) to:
- Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred.

- Gamble.
- Undertake political lobbying.
- Promote or run a commercial business.
- Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright.
- Send emails, texts or messages or publish anything on a website, social networking site or blog, which:
  - Is critical about members of the school community, including pupils.
  - Contain specific or implied comments you would not say in person.
  - Contain inappropriate comments which could cause offence or harassment on the grounds. of gender, race, disability, age, religion or sexual orientation.
  - Has originated from a chain letter.
- Conduct private and intimate relationships via email.
- Spend school time on personal matters (e..g arranging a holiday, shopping, looking at personal interest websites). This may be treated as fraud.
- Store personal information on the school network (e.g. personal photos, screensavers or wallpaper).
- Download or copy software (excluding software updates).
- Use the email system to transmit any documents or software without checking the copyright or licence agreement.
- Install software licensed to the school on a personal computer unless permission to do so is explicitly covered by the school licence agreement.
- Take, transmit or publish pictures of a member of staff or pupil on your mobile phone, camcorder or camera without the person's permission.
- Give away email lists for non-school business.
- Use internet chat rooms (other than the secure, moderated facilities which are provided within the school's learning platform).

Monitoring and privacy

The school's email and internet facilities are business systems, owned by the school. The school therefore reserves the right to monitor all use of the internet and of the school's ICT systems in line with guidance. Usage will be monitored to ensure that the systems are being employed primarily for business and educational reasons, that there is no harassment or defamation taking place and that employees are not entering into illegal transactions.

- Staff need to be aware that internet sites visited are traceable, and that deleted or trashed messages or attachments can be recovered.

- Email, telephone calls and internal and external post (unless clearly identified as private and confidential post) should be used primarily for business and educational purposes.

- School managers have proxy access to all the school's communication systems for monitoring and interception of communications in order to deal with matters in an employee's absence for holiday, illness or other reason.

- Any material stored on the school's network or being circulated via the school's email system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) monitoring or surveillance without an employee's knowledge can be carried out on internal email systems or information stored on a server.

Breaches and sanctions of this policy
Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action against you in accordance with the school's disciplinary policy.

Where breaches involve third parties, including pupils, parents or other individuals, the police will be involved as appropriate and the Guidelines on prosecuting cases involving communications sent via social media (CPS, revised 2018) will be used.

Monitoring and evaluation

The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the governors' rolling programme of reviews.

Next review due: March 2025.