



# Hopelands Preparatory School

38/40 Regent Street, Stonehouse, Gloucestershire, GL10 2AD

## **Acceptable use of ICT, Mobile Phones and Other Electronic Devices Policy**

### **SCOPE OF POLICY**

**This policy applies to the school including the EYFS. The policy applies to all staff at all levels (teaching and non-teaching) at Hopelands School, whether directly employed or agency, all Governors, all volunteers and all contractors.**

**This policy must be read in conjunction with the remote learning policy and KCSiE 2023**

#### **Computer network**

- Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, racist, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will result in disciplinary action.
- Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action.
- You are responsible for the security of your passwords.
- The network must not be used for commercial purposes, e.g. buying or selling goods.
- Any software that is installed must be covered by the appropriate licensing agreements.
- Copyright of materials available on the network must be respected.

#### **Internet / Email**

- Use of the internet and email must be solely for legitimate school purposes.
- Use of the internet and email are subject to scrutiny by the school's filtering provider. Any action that might damage the good reputation of the service will be dealt with as a serious act of misconduct.
- Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Emails sent from school should contain the same professional levels of language and content as applied to letters or other media.
- You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email.
- All staff should avoid contacting pupils on social networking sites. This is to avoid any possible misinterpretation of motives and the risk of any allegations being made. Students must not be added to social media sites for staff.

#### **Use of photographs, video and digital images**

- Staff **must** only use school equipment to record, or take photographs of pupils, and only then if the relevant permission has been obtained.

## **Mobile Phones**

### **Use of Work Mobile Phones during the working day**

- Professional tone to be used in all phone calls made and text messages sent using work phones. Personal calls, other than in an emergency, are forbidden on work phones.
- Calls and contact to pupils and parents should be restricted to the hours of 8.00 am to 6.00 pm and only using school telephones or school mobile telephones. Staff must not share their personal contact details.
- Direct contact with pupils by telephone calls or text messages is limited to essential service needs only.

### **Use of Personal Mobile Phones during the working day**

- To ensure the safety and welfare of the pupils in our care personal mobile phones, cameras and video recorders must not be used when children are present.
- All mobile phones must be kept in a secure place (not in a pocket), switched off and not be accessed throughout contact time with the children.
- In exceptional circumstances, which have been discussed and agreed with a member of the leadership team, staff may keep their phone switched on and accessible as long as they use their phone out of view of children, i.e. in a room designated for staff, e.g. the staff room or an office.
- During school visits mobile phones should be used away from the children and for emergency purposes only.
- Photographs or images of any children within our care may only be taken following parental consent and only using one of the school cameras / IT equipment. These images should remain within this setting or be shared only with the parents of the child concerned.
- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. **ONLY** school property can be used for this.
- School photographs and recordings can only be transferred to and stored on a school computer.
- Children are not allowed to have mobile phones in school. If children bring a phone to school, they should take it to the school office where it will be kept until the end of the school day.
- Children have their photographs taken to provide evidence of their achievements for their development records (The Early Years Foundation Stage, EYFS 2007).
- Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day.
- Employees accessing emails using either their personal or business mobile phones should have the appropriate secure systems in place to ensure should their phone be lost or stolen the data cannot be accessed without a password or pin.
- Employees should not access social networking sites via their mobile phones (business or personal phones) during working hours.
- Employees should not provide parents or pupils with their personal mobile phone number.

## **Social Media**

Social Media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave teachers vulnerable if they fail to observe a few simple precautions. This policy is designed to protect school staff and pupils from potential harm or from becoming victims of radicalisation, extremism and malicious, upsetting or inadvisable contact. (For detailed explanations please see the School Safeguarding Policy)

- Staff members **must not** identify themselves as employees of the school in their personal web space apart from professional websites such as LinkedIn. This is to prevent information on these sites from

being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

- Staff members **must not make contact through any personal ICT or social medium with any pupil**, whether from our school or any other school, unless the pupil\* is your own family member OR an existing close family friend. School does not expect staff members to discontinue contact with their own family members or significant family friends via personal social media, however care should be taken not to communicate with friends of the family member who may be school pupils.
- Staff **must not have social media contact with any pupils' family members (parents/carers)** This is in-line with the NASUWT teachers' union and other unions which say that teachers should never under any circumstances accept Facebook friend requests from parents of a pupil.
- If staff members need to communicate with pupils for work purposes, they can only do so through the official school email or school mobile 'phone. Personal email addresses/phone numbers **must not** be shared with pupils or parents.
- Staff members **must decline 'friend requests' from pupils** they may receive in their personal social media accounts. Pupils/parents will be informed that this will be the case on induction.
- On leaving school employment, staff members **must not** contact pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.
- Any information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, County Council staff and other parties and service or County Council corporate information must not be discussed on their personal webspace or social media sites.
- Photographs, videos or any other types of image of pupils and their families or images depicting staff members who can be identified as school staff must not be published on personal webspace or social media sites.
- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.
- School logos or brands must not be used or published on personal webspace/social media sites (apart from professional websites such as LinkedIn)
- School does not permit personal use of social media or the internet during core contracted work hours. Access to social media sites for personal reasons is not allowed between 9am and 4.15pm (apart from during lunch breaks). Staff members are expected to devote their contracted hours of work to their professional duties.
- **Caution** is advised when inviting work colleagues to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place. Staff **must not** use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations.
- Staff members **are advised to set the privacy levels of their personal social media sites as strictly as they can** and to opt out of public listings on social networking sites to protect their own privacy. Staff

members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

**BREACHES OF THE POLICY**

- Any breach of this policy may be investigated and may lead to disciplinary action being taken against the staff member/s involved in line with School Disciplinary Policy and Procedure.
- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school liable to third parties may result in disciplinary action or dismissal.
- Contracted providers of the school must inform the relevant service immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service. Any action against breaches should be according to contractors' internal disciplinary procedures.

*If you are in doubt about any of the above, please seek advice.*

**I have read and accept the terms of the: -**

**ICT, Technology and Social Media Acceptable Use Policy for all Permanent and Temporary Staff**

*Please tick to confirm you have read this policy*

**I understand the implications of any breach of this policy as outlined above.**

Name (Printed): \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

This policy was adopted at a meeting of

Held on

September 2023

Date to be reviewed

September 2024

Signed on behalf of the senior management team

Name of signatory

Sonja Jones

Role of signatory

Joint Head

Signed on behalf of the Governing Body

Name of signatory

Richard James

Role of signatory

Chair of Governors

