



## **Houghton Regis Primary School**

# **Internet, E-mail and Social Networking Policy**

This policy provides the acceptable standards for the use of the Internet, e-mail and social-networking for all school employees at Houghton Regis Primary School. It applies to all school employees, peripatetic teachers, visiting staff, volunteers and casual workers. This policy should be read in conjunction with Guidance for Safer Working Practice for Adults who work with Children and Vulnerable People and the Code of Conduct Policies.

This policy covers the use of the Internet and e-mail, as well as all Social Networking Sites and Applications, such as, but not limited to Twitter, Facebook, You Tube, Bebo, My Space etc. It further includes: Blogging, online discussion groups or social networking groups.

### **Purpose**

The purpose of this policy is to:

- Set out clear guidance of the acceptable use of the Internet, e-mail and social networking sites
- Ensure confidentiality of the school, staff and pupils is maintained at all times
- Ensure that all school employees understand the consequences of failing to comply with the Internet, E-mail and Social Networking Policy
- Ensure the appropriate use of the school's resources

### **Responsibilities**

#### **Governing Body/Headteacher responsibilities**

Bedford Borough Council will provide guidance on updating this policy as and when appropriate.

It is the responsibility of the Headteacher to publicise and make this policy available to all current and future school employees, and to ensure that the standards within it are both monitored and enforced and to advise the Governing Body of any serious breaches of this policy.

It is the responsibility of both the Governing Body and the Headteacher to take corrective and disciplinary measures as are necessary when a breach of this standard occurs and to contact and co-operate with police and other law enforcement agencies where a breach of these standards may constitute a criminal act.

#### **Employee's responsibilities**

It is the responsibility of the school employee to read and comply with the Internet, E-mail and Social Networking Policy. School employees are reminded that they are bound by the School's Code of Conduct and Teaching Staff are further subject to the Teachers Standards Document.

Under the Safeguarding Vulnerable Groups Legislation 2006 school employees may be referred to the Disclosure and Barring Service (DBS) where the school has significant concerns or suspicions about an employee's conduct or behaviour.

## **Email Use**

E-mail is provided for business use. It is not a perk or means of entertainment. Content of all e-mails should be substantially related to workplace matters.

Email should never be sent, forwarded or replied to where the content is adult, explicit offensive or otherwise inappropriate as specified in table 1.1 below.

**Table 1.1 Inappropriate e-mail content definitions**

<b>Abusive</b>	<b>Bullying</b>	<b>Defamatory</b>
<b>Disruptive</b>	<b>Harmful to Council, LA or School morale</b>	<b>Harassing</b>
<b>Insulting</b>	<b>Intolerant</b>	<b>Obscene</b>
<b>Offensive*</b>	<b>Politically biased**</b>	<b>Sexual innuendo</b>
<b>Violent</b>	<b>Threatening</b>	
<b><i>*Prohibited material will include any material which may be construed as offensive on the grounds of gender, race, ethnic origin, disability, sexuality, religion, trans-sexualism, gender re-assignment, age, HIV status, size, stature, trade union membership/office or any combination thereof.</i></b>		
<b><i>**As school employees we must not demonstrate partiality for or against any political grouping or individual (this will not apply to union officials fulfilling an obligation on behalf of their professional association).</i></b>		

## **Internet Use**

Access to the Internet is similarly provided for business use. It is not a perk or means of entertainment. Sites and groups visited should be related to workplace matters. The following relates specifically to use of school property for personal purposes.

Sites must not be accessed which contain inappropriate material as defined in Table 1.2.

**Table 1.2 Inappropriate web content definitions**

Adult or explicit (including photo searches for such material)	Incitement (e.g. race hate or supremacist ideologies)
Chat rooms or Instant Messaging ( <i>except for educational purposes e.g. NCSL, BECTA or Grid Club</i> )	Personal ads or dating
Criminal skills or resources	Newsgroups and forums ( <i>except for educational purposes</i> )
Downloads of ring-tones, screensavers and games	Internet based Peer to peer networks e.g. Napster etc.
Downloads of freeware, shareware or evaluation packages ( <i>excepting by authorised persons as designated by the school and in compliance with copyright law</i> )	Hacking, virus writing or password cracking
Illegal drugs	Tasteless and offensive content such e.g. jokes, pictures or profanity
Gambling	Depiction or advocacy of violence or the use of weapons
Social Networking sites  (see below)	Facebook, My Space, You Tube* etc

\* 'The use of YouTube is not permissible, however, video clips may be downloaded and stored on the server for use in the class'

### **Personal Use of Internet and Email**

Facilities and equipment that are provided by the school and used by employees as part of their normal duties must not be abused by employees for their own private benefit or gain.

This will cover all school property, for example telephones, computers, tools, fax machines, paper etc. Council property should not be taken home, or taken away from the normal place of work, unless prior permission has been given by an employee's immediate line manager or unless these are acceptable resources to fulfil the contractual requirements of the job at home (for example planning, preparation and marking).

- The sending of e-mails that are, wholly or substantially unrelated to School business should be restricted to out of school hours and designated breaks.
- Access to Internet web sites that are unrelated to School business should be restricted to out of School hours and designated breaks.
- Personal use of both e-mail and the Internet must not breach any of the definitions of inappropriate use as defined in this document.
- Access to Social Networking sites is not permissible on the school premises at any time other than on designated breaks.

### **Conducting financial activities on the Internet**

While this policy does not specifically ban the use of the Internet for conducting personal financial transactions e.g. E-banking, we warn against it. Residual information from such activities can be left on your computer hard drive and could subsequently be accessed by others. Neither the School, the LA, nor the Council accept any liability for any resulting loss or damage.

### **Safeguarding Children**

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. Employees must abide by agreed methods of communication within school. Adults should ensure that all communications are transparent and open to scrutiny.

Safeguarding children is the responsibility of all school employees. The key principles are:

- School employees **must not** communicate, (including accepting 'friend' requests) with any current pupils of the school, or from any other educational establishment, on social networking sites such as Facebook. This is applicable **even** if a school employee has permission from a pupil's parent/guardian. (This would not apply to current pupils that an individual employee is directly related to, e.g. their child, niece or nephew). School employees should not communicate with, including being 'friends' with, past pupils whilst they are below the age of nineteen.

These principles apply:

- Regardless of whether access occurs during or outside of contracted work hours.
- To all technology whether provided by the school or owned by the employee.

### **Unacceptable use of Social Networking Sites/Applications**

Through Social Networking Sites/Applications, school employees **must not**:

- Disclose private and confidential information relating to pupils, parents, other school employees, their employment directly or the school

- Discuss or reveal any matters relating to the school, school employees, pupils or parents
- Identify themselves as a representative of the school.
- Write abusive comments regarding school employees, pupils or parents/guardians
- Harass or bully school employees, persons unrelated or related to the school through cyber bullying and social exclusion
- View or update their personal site (on Facebook, twitter etc.) during the working day, unless on a designated break. (This includes via work or mobile telephone and/or IPAD).
- Use school equipment/devices to access such sites.
- By proxy update their personal site (Facebook, twitter etc.) during their normal working day, and must ensure that their social networking site/application is secure at all times from third parties
- Access or share illegal material
- Publish any content, which may be deemed as defamation or discrimination
- Post any images of pupils from the school or any other previous educational establishment where the employee has worked.
- Without permission post any images of school employees on social networking sites from the school or any other previous educational establishment where the employee has worked.
- Set up and/or use an alias social networking account to circumvent the policy
- Breach any of the schools other policies and procedures such as the School's Code of Conduct, Bullying and Harassment Policy, Equalities Policy
- Use it as a forum for raising and escalating concerns regarding the school or the Council. These concerns should be raised using the Whistle Blowing Procedure.

This list is not exhaustive

### **Consequences of breaching the standards laid out in this policy**

The use of school equipment to access e-mail in order to send, view or store other inappropriate content (as defined in table 1.1) or provision of an e-mail address to a 3<sup>rd</sup> party with the intention of receiving inappropriate content will constitute misconduct or gross misconduct.

The use of school equipment to deliberately access inappropriate web content (as defined in table 1.2) will constitute misconduct or gross misconduct.

The use of school equipment to deliberately and repeatedly access such material will constitute gross misconduct.

The use of e-mail or the Internet, including social networking sites, for the preparation, commission or abetting of a criminal act will constitute gross misconduct.

The use of personal equipment during school hours, including designated breaks, in any breach of these standards is also likely to result in the consequences listed above and employees must also consider the consequences of doing so outside of school hours.

It is with this in mind that all school employees are reminded that:

**Everything posted online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed. Therefore, assume that everything that is written is permanent and can be shared.**

School employees are reminded that they should at all times:

- Have the highest standards of personal conduct (inside and outside of School)
- Ensure that their behaviour (inside and outside of School) does not compromise their position within the school
- Ensure that their judgment and integrity should not be able to be brought into question.

Any failure to abide by the Internet, e-mail and Social Networking Policy will result in disciplinary action.

School employees must alert the Governing Body and/or Headteacher where a breach of these standards is suspected or known to have occurred. Failure to do so may result in disciplinary action.

### **All schools staff responsibilities**

Employees must adhere to these standards in following circumstances:

- When working on schools premises or when out on school trips
- When using equipment and utilities (hardware, software or e-mail and internet access) provided by the School, the LA or Central Bedfordshire Council at home or other locations

The standards apply regardless of whether access occurs during or outside of contracted work hours.

Employees must alert the Headteacher or a relevant senior member of staff where breach of these standards is suspected or known to have occurred.

### **Monitoring and reporting**

The school and Central Bedfordshire Council or their agents will monitor use of the Internet and e-Mail.