



EAST ANGLIA SCHOOLS TRUST

INTERNET & EMAIL USAGE POLICY

Chair of Governors/Board of Directors signature:

.....

Date:

Next Review Date: Autumn term 2018

Internet & Email Usage in Schools Policy

1. Purpose of this guidance

1.1 This guidance is for all staff who use the Trust facilities for internet and email. It should be read in conjunction with the Trust's E-Safety Policy and Acceptable Use Policy.

1.2 This guidance aims to advise staff of the following:

- Safe and secure internet and email use
- Acceptable use of equipment
- Policy on social networking sites
- Relevant legislation
- The consequences of improper/unacceptable use of the internet, email and equipment

2. Introduction

2.1 The virtual world opens up new opportunities for teaching and learning. However school staff need to be aware of the risks attached to its use and the need to comply with the Trust policy. This policy requires that all Internet connections must be arranged via Trust approved providers. Local Area Network (LAN) security is the responsibility of the Trust. Schools must ensure that security and their information systems are regularly reviewed and that protection against viruses is installed and regularly updated.

2.2 Information Technology includes a wide range of systems including mobile 'phones, tablets, digital cameras, email and internet use.

2.3 The Trust's E-Safety and Acceptable Use Policies require that school staff sign a Code of Conduct for ICT which explains how to use school ICT facilities and equipment responsibly and appropriately.

3. **Safe and secure internet and email use, and appropriate use of equipment**

The Schools Code of Conduct for ICT covers the following points regarding safe and secure internet and email use:

- 3.1 School ICT equipment, systems and data stored on them remain the sole property of the school whether used on or off the premises.
- 3.2 School information systems and equipment may not be used for private purposes.
- 3.3 The Head of School or Trust information Technology Coordinator will provide clarification of what constitutes permitted use where questions arise.
- 3.4 Staff must ensure that all electronic communications made reflect the professional nature of responsibilities. This follows expectations for Professional Standards.
- 3.5 Staff use of school information systems, internet and email is monitored and recorded to ensure policy compliance.
- 3.6 Personal ICT devices should not be connected to the School systems to ensure data security and virus protection.
- 3.7 Staff must not install any software and hardware on school ICT equipment.
- 3.8 Staff must not disclose or share any password or security information with anyone other than authorised ICT staff.
- 3.9 Staff must not leave their computers logged on and unattended in situations where this creates a risk of unauthorised people accessing sensitive information.
- 3.10 Staff must ensure that personal data is stored securely with encryption whether in school, taken off the school premises or accessed remotely.
- 3.11 Staff must comply with copyright and intellectual property rights as defined by UK and EU law.
- 3.12 Staff must report any incidents of concern regarding inappropriate use of ICT systems or equipment to the school ICT leader, E-Safety Coordinator, a Designated Safeguarding Officer or Head of School.

4. **Social networking sites**

- 4.1 Staff must not access social networking sites for personal use via school information systems or using school equipment.
- 4.2 Staff are discouraged from using social networking sites. Where staff do use social networking sites, they should not publish specific and detailed private thoughts. If staff make the choice to access social networking sites using their personal systems and equipment, due care must be taken to maintain the professional standing and reputation of both the school and individual. For example, work related information, names or details must not be shared.

- 4.3 In addition staff must not place inappropriate photographs on any social network
- 4.4 Staff must not communicate with students and parents over social network sites using their personal systems and equipment. They must block unwanted communications.
- 4.5 In addition the internet should not be used for the following activities:
- Conducting illegal activities
 - Accessing or downloading pornographic material
 - Gambling
 - Soliciting for personal gain or profit
 - Managing or providing a business or service
 - Revealing or publicising proprietary or confidential information
 - Representing personal opinions as those of the school
 - Making or posting indecent remarks or proposals
 - Sharing ideologies or activities coming under the scrutiny of the PREVENT agenda.

5. **Legislation**

The following legislation must be considered by staff when using the internet or email.

5.1 **Human Rights Act 1998**

The Human Rights Act 1998 provides the "right to respect for private and family life, home and correspondence". This is enforceable against public sector employees including schools staff.

5.2 **Regulation of Investigatory Powers Act 2000 (RIPA)**

Covert monitoring is unlawful unless undertaken in accordance with RIPA and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. RIPA covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for unlawful interception of communications.

There are two areas where monitoring is lawful. These are:

- Where the school believes that the sender and intended recipient have consented to the interception
- The school can monitor without consent in the following circumstances (in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000: to ensure compliance with regulatory practices; to ensure standards of service are maintained; to prevent or detect crime; to protect the communication system (including unauthorised use and risk of viruses); and to pick up messages when someone is away from school.

The Head of School should make all reasonable efforts to ensure users know that communications may be intercepted and monitored. For example, through the use of profanity filters. The Head of School will be informed where staff or pupils fail to follow this policy.

5.3 **Data Protection Act 1998**

The Data Protection Act 1998 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. The Act states that anyone processing personal data must comply with the eight enforceable principles of good practice. These state that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

5.4 **Freedom of Information Act 2000**

The Freedom of Information Act 2000 deals with access to official information, giving individuals and organisations the right to request information held by a public authority. The Act requires public authorities to have an approved publication scheme, detailing the specific information they hold and how this can be accessed. The Information Commissioner's Office (ICO) is the UK's independent authority set up to promote access to official information and to protect personal information. The website contains specific information and guidance for schools and education, including:

- Accessing pupils' information
- Accessing official information
- Individuals' rights of access to examination records
- Disclosing students' exam results to the media
- Taking photos in schools
- Use of biometrics in schools.

5.5 **Copyright, Designs and Patents Act 1988, amended by the Copyright and Related Rights Regulations 2003**

This legislation covers intellectual property (IP) - the outcome of thought or intellectual effort. IP rights protect people against unauthorised use of their inventions, designs, brand names or original creations. The rights include patents, trademarks and copyright. Of the IP rights, copyright has the most relevance for schools. Copyright material on the internet is generally protected in the same way as material in other media. Each web page may contain several different copyrights if it contains text, music and graphics. The exceptions which apply to hard copy materials tend to also apply to material on the internet, e.g. for non-commercial research or private study.

Most websites have a copyright statement, but if permitted uses are unclear, staff must seek permission directly from the owner of the website. Unauthorised use can be a criminal offence equivalent to theft.

5.6 **Computer Misuse Act 1990, amended by the Police and Justice Act 2006**

The Computer Misuse Act 1990 deals with criminal acts committed using a computer. The Police and Justice Act 2006 brings it up to date with developments in computer crime and allow for tougher penalties. Offences include unauthorised access to computer material; unauthorised acts to impair operation of computer; making, supplying or obtaining articles for use in computer misuse offences; acting with intent to hinder access to any program or data held in any computer; and acting with intent to impair the operation of any such program or the reliability of such data (e.g. hacking or denial of service attacks).

5.7 Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These Acts are concerned with material that might be criminal, cause harm to young people or be otherwise unlawful.

6. The consequences of improper/unacceptable use of the internet, email and equipment

6.1 The use of Information Technology Systems in each school is monitored and this includes the right of the Head of School to intercept email and delete inappropriate materials where he or she believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes, or for storing unauthorised text, imagery or sound.

6.2 Staff must be aware that improper or unacceptable use of the internet, email and equipment could result in legal proceedings and the use of the school's Disciplinary Procedure. Sanctions will depend upon the gravity of misuse, and could result in dismissal.

CHANGE LOG		
<i>CHANGES MADE</i>	<i>DATE</i>	<i>NEW VERSION NUMBER</i>
1.2 Policy on Social networking	12/11/2015	2.0
2.1 Deletion of Norfolk County Council and change to Trust	12/11/2015	2.0
2.2 update technology references	12/11/2015	2.0
3.1 addition of sole property	12/11/2015	2.0
3.4 addition of professional responsibilities	12/11/2015	2.0
3.6 – no personal systems to be connected	12/11/2015	2.0
3.7 deletion and addition of ICT equipment	12/11/2015	2.0
3.11 addition of UK and EU law	12/11/2015	2.0
3.13 Deleted	12/11/2015	2.0
4.1 Deleted	12/11/2015	2.0
4.2 addition of ned for due care to reputation	12/11/2015	2.0
4.5 Deleted	12/11/2015	2.0
New 4.5 addition PREVENT duty	12/11/2015	2.0
5.2 addition of profanity filter guidance	12/11/2015	2.0
6.1 Amended - monitoring of Information systems	12/11/2015	2.0
Logo and name on front page changed to EAST	03/10/2017	2.1