# Acceptable Use Policy for Schools and Academies

**Effective from September 2011**

## 1. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within a school or educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

i) the steps taken in school to ensure the-Safety of pupils when using the internet, e-mail and related technologies

ii) the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school

iii) the school's expectations for the behaviour of staff when accessing and using data.

## 2. Scope of policy

The policy applies to all school based employees, including individuals working in a voluntary capacity. All schools are expected to ensure that non-employees on site are made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the school/educational settings' disciplinary procedures and code of conduct applicable to employees and pupils.

Where this policy is applied to the Head Teacher, the Chair of Governors will be responsible for its implementation.

Where the Governing Body wishes to deviate from this proposed policy or adopt any other policy, it is the responsibility of the Governing Body to arrange consultation with appropriate representatives from recognised trade unions and professional associations.

## 3. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

- The Children Act 2004
- School Staffing (England) Regulations 2009
- Working Together to Safeguard Children 2010
- Education Act 2002

This document is only available to schools that have an SLA for HR advisory services with LGSS. The copying, publishing, sharing or distribution of this document is unauthorised without the express written permission of the LGSS HR Business Partner for Schools.

- Safeguarding Vulnerable Groups Act 2009
- Data Protection Act 2018

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to the legislation listed above.

## 4. Responsibilities

### Head Teacher and Governors

The Head teacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head Teacher and Governors should:

- designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school.
- provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.
- promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.
- share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- ensure that e-safety is embedded within all child protection training, guidance and practices.
- elect an e-Safety Governor to challenge the school about e-Safety issues.
- make employees aware of the LSCBN Inter-agency Child Protection Procedures at www.lscbnorthamptonshire.org.uk

### E-Safety Lead

The nominated e-Safety lead should:

- recognise the importance of e-Safety and understand the school's duty of care for the-Safety of their pupils and employees.
- establish and maintain a safe ICT learning environment within the school.
- ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- with the support of the Network Manager or IT Subject Leader, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.
- report issues of concern and update the Head Teacher on a regular basis.
- liaise with the Anti-Bullying, Child Protection and ICT leads so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.
- co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.


The copying, publishing, sharing or distribution of this document is unauthorised without the express written permission of the LGSS HR Business Partner for Schools.

- maintain an e-Safety Incident Log to be shared at agreed intervals with the Head Teacher and Governors at governing body meetings.
- with the support of the Network Manager or ICT Lead, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate (School must decide how they wish to do this-i.e. monitor upon concern raised, random monitoring through collection of devices, or purchase of specialist monitoring software e.g. Securus)

**Individual Responsibilities**

All school based employees, including volunteers under the age of 18, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.
- report any e-Safety incident, concern or misuse of technology to the e-Safety lead or Head Teacher, including the unacceptable behaviour of other members of the school community.
- use school ICT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.
- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.
- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.
- understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out, should be detailed in the school's local IT Policy.
- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

## 5. Inappropriate Use

**In the event of staff misuse**


The copying, publishing, sharing or distribution of this document is unauthorised without the express written permission of the LGSS HR Business Partner for Schools.

If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head teacher/Safeguarding lead immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- Schools Senior HR Advisory Team
- LADO (Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the e Safety Incident Flowchart within the accompanying Employee Handbook for further details.

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

**Examples of inappropriate use**

- Accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

**Inappropriate use by a child or young person**

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. Template student Acceptable Use Rules and example sanctions can be found in the appendix.

Students should recognise the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with employees.

## 6. Policy Review

The Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable Use Rules for students should be consulted upon by the student body to ensure that all young people can understand and adhere to expectations for online behaviour.

## 7. Data Protection

Any data collected as part of employing and managing employees is held securely. It is accessed by, and disclosed to, individuals only for the purposes of completing that specific procedure; process or activity.

Records are retained and destroyed in accordance with the organisations Retention Schedule.

Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the organisation's Data Protection Policy immediately. It may also constitute a disciplinary offence, which may be dealt with under the Disciplinary Procedure.

## 8. Useful Links


The copying, publishing, sharing or distribution of this document is unauthorised without the express written permission of the LGSS HR Business Partner for Schools.

**NASUWT** Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

**NUT** E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

**UNISON**- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786


The copying, publishing, sharing or distribution of this document is unauthorised without the express written permission of the LGSS HR Business Partner for Schools.