RUSKIN INFANT SCHOOL AND NURSERY

Acceptable Use Policy

Revised: December 2019

Revised by: Ben Morris

To be reviewed by: September 2020

This school policy reflects the consensus of opinion of the whole teaching and support staff and has the full agreement of the governing body.

1. Policy Statement

In order to create a safe learning environment for children, effective policies and procedures which are clearly understood and followed by all staff 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. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within Computing.

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

i) the steps taken at the school to ensure the safety of children when using the internet and online technologies

ii) the school's expectations for the behaviour of all users whilst accessing the internet or online technologies within and beyond the 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 technologies and the internet is used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the school 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 another policy, it is the responsibility of the Governing Body to arrange consultation with appropriate representatives from recognised trade unions and professional associations.

3. Privacy

The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the

school stores on its network regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.

The school will only process data in line with its lawful basis to uphold the rights of botpupils and staff and other third parties.

In order to protect pupils' safety and wellbeing, and to protect the school from any third party claims or legal action against it, the school may view any data, information or material on the school's ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services.

4. 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
- Working Together to Safeguard Children 2018
- Education Act 2002
- Safeguarding Vulnerable Groups Act 2009
- School Staffing (England) Regulations 2009

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

5. Responsibilities

Head Teacher and Governors

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

- designate an online safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring online safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school.

- provide a safe, secure and appropriately filtered internet connection for staff, children and young people within the school.

- provide resources and time for the online safety lead and employees to be trained and update protocols where appropriate.

- promote online safety across the curriculum and have an awareness of how this is being developed, linked with school development plans.

- ensure that any equipment which holds sensitive or confidential information and leaves the school premises (e.g. iPads, staff laptops and memory sticks) is encrypted to ensure GDPR is met.

- share any online safety progress and updates at all staff meetings and ensure that all present understand the link to child protection.

- ensure that online safety is embedded within all child protection training, guidance and practices.

- select an online safety governor to challenge the school about online safety issues.

- make employees aware of the LSCBN Inter-agency Child Protection Procedures at www.lscbnorthamptonshire.org.uk

- Ensure all staff, volunteers, students and committee members have read, understood and signed to say that they will adhere to the Acceptable Use Policy. This must be reviewed in an appropriate timescale.

Online safety Lead

The nominated online safety lead should:

- recognise the importance of online safety and understand the school's duty of care for the safety of their pupils and employees

- establish and maintain a safe Computing learning environment within the school.

- ensure that all individuals in a position of trust who access technology with children understand how filtering levels operate and their purposes.

- with the support of the IT Support provider/Technician, ensure that filtering is set to the correct level for all staff, volunteers and children accessing school equipment.

- report issues of concern and update the Head Teacher on a regular basis.

- co-ordinate and deliver employee training according to new and emerging technologies so that the correct online safety information is being delivered.

- maintain an online safety Incident Log to be shared at agreed intervals with the Head Teacher.

- with the support of the Network Manager, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate. This will be randomly monitored through monitoring website activity and random collection of devices.

- liase with the Anti-Bullying, Child Protection and Computing lead so that procedures are updated and communicated, and take into account any emerging online safety issues and technological changes.

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 their use of technology meets expectations in line with GDPR

- ensure they adhere to the code of conduct policy which outlines acceptable use of technology including use of social media

- 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 online safety incident.

- report any online safety incident, concern or misuse of technology to the online 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 child data or images of children. 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 others or be incompatible with their professional role. Individuals working with children must understand that behaviour in their personal lives may impact upon their work with those children 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 schools online 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.

6. Inappropriate Use

In the event of staff misuse

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 immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

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

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

- 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.

- Accepting parent's as 'friends' on social networking sites, or exchanging personal email addresses or mobile numbers when there is no previous relationship.

- Accepting or requesting children as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

7. Policy Review

The Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure and Computing developments. Acceptable Use 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.