***Policy & Procedure***

Newcroft

Primary Academy

Aspiring for Excellence

# Newcroft Primary Academy

# E Safety Policy

# *2016-2019*

This policy is reviewed every three years and was agreed by the Governing Body of Newcroft Primary Academy in Autumn 2016 **and will be reviewed again in Autumn 2019**

Signed: _____ Chair of Teaching and Learning

Date: _____

## *Non-Statutory Policy*

***Newcroft Primary Academy***

***E Safety Policy***

## Aims and Vision


**Our aim** is that all children at Newcroft become creative, active and reflective learners through consistent focus upon:

The aims of this policy are:

- To keep everyone safe online
- To help develop a culture of openness amongst everyone
- To comply with legislation

### Writing and reviewing the E-safety policy

- The E-safety Policy relates to other policies including those for Curriculum, Teaching and Learning, Behaviour, Anti-Bullying and Safeguarding.

- The Head of School and Computing Leader have the overview for E-safety in the school.

- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.

### Teaching and learning

### Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- The Internet use is a part of the curriculum and a necessary tool for staff and pupils. The benefits of using the Internet in education include:

    - access to world-wide educational resources including museums and art galleries;
    - educational and cultural exchanges between pupils world-wide;
    - cultural, vocational, social and leisure use in libraries, clubs and at home;
    - access to experts in many fields for pupils and staff;
    - staff professional development through access to national developments, educational materials and good curriculum practice.

- The school Internet access is provided by Schools Broadband and includes filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet

- Pupils will be shown how to publish and present information appropriately to a wider audience.

**Pupils will be taught how to evaluate Internet content**

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and they will be shown how to validate information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector (and by immediately reporting concerns to an adult in their class)

**Managing Internet Access**

**The IT Coordinator will**

- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents;

- Promote an awareness and commitment to e-safeguarding throughout the school community;

- ensure that e-safety education is embedded across the curriculum;

- liaise with school IT technical staff;

- communicate regularly with SLT and the designated e-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;

- ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident.

**Information system security**

- School IT systems security will be reviewed regularly

- Virus protection will be updated regularly

- Security strategies will be discussed with the Local Authority

**E-mail**

- Pupils and staff may only use approved e-mail accounts on the school system (those ending in @newcroft.leics.sch.uk).

- Pupils must immediately tell a teacher if they receive offensive e-mails or other messages

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Staff to pupil email communication must only take place via a school email address and will be monitored.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school will consider how e-mail from pupils to external bodies is presented and controlled.

**Published content and the school web site**

- The contact details on the Website are the school address, e-mail and telephone number. Staff or pupils personal information will not be published. The contact us pages directs emails to the Head teacher.

- The Head of School will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing photographs, images and work**

- Photographs that include pupils will be selected carefully and will only include pupils for whom permission has been granted by parents.

- Pupils' full names will not be published on the Website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs or images of pupils are published

- Written permission from adults will be obtained before their names, photographs or images of themselves are published

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

**Social networking and personal publishing on the school learning platform**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.

- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

- Pupils must not place personal photos on any social network space without permission.

- Pupils, parents and staff will be advised on the safe use of social network spaces (those appropriate for primary pupils)

- Pupils will be advised to use nicknames and avatars when using social networking sites.

**Managing filtering**

- The school will work in partnership with Primo IT to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to a known adult and then the nominated member of staff.
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing videoconferencing**

- If used, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

**Other devices**

- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).
- The school ipads will be managed carefully and pupils' use of them will be for solely educational purposes.

**Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**Policy Decisions**

**Authorising Internet access**

- All staff must read and sign the 'Staff Code of Conduct for IT' before using any school IT resource (appendix 1 of this policy)

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

- Parents will be asked to sign and return a consent form.

**KS2 Pupils must agree to comply with the Acceptable Use Policy (Appendix 2) before being granted Internet access.**

- Any person not directly employed by the school will only be allowed supervised access to the school's IT systems (other than trainee teachers).

**Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Leicestershire County Council can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit IT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

**Handling E-safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Head teacher.

- Complaints of a child protection nature must be referred to the Safeguarding Lead and dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

**Community use of the Internet**

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

**Communicating/ Introducing the E-safety policy to pupils**

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

**Staff and the E-safety policy**

- All staff will be given the School E-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues**.**

**Enlisting parents' support**

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents (of pupils in KS2) to sign the parent/pupil Acceptable Use Policy when they register their child with the school.

***Equality Statement***

At Newcroft Primary Academy, we actively seek to encourage equity and equality through our teaching. As such, we seek to advance the equality of opportunity between people who share any of the following characteristic:

- gender;
- ethnicity;
- disability;
- religion or belief;
- sexual orientation;

- gender reassignment;
- pregnancy or maternity.

The use of stereotypes under any of the above headings will always be challenged.

**Inclusion**

Our school is an inclusive school. We aim to make all pupils feel included in all our activities. We make all our teaching fully inclusive. We recognise the entitlement of all pupils to a balanced, broadly-based curriculum. We have systems in place for early identification of barriers to their learning and participation so that they can engage in school activities with all other pupils. We acknowledge the need for high expectations and suitable targets for all children.

Appendix 1

# Staff Code of Conduct for IT

**To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.**

 I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.

 I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.

 I understand that school information systems may not be used for private purposes without specific permission from the headteacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

 I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

 I will respect copyright and intellectual property rights.

 I will report any incidents of concern regarding children's safety to the e-Safety Coordinator (Lorraine Lloyd), the Safeguarding Lead (Carole Atkinson) or Head of School (Lizzie Hallam).

I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

 I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it 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 or unlawful text, imagery or sound.

**I have read, understood and accept the Staff Code of Conduct for IT.**

Signed: …… Name: …….…… Date: ……..……

Accepted for school (signed): …… Name

Appendix 2

# Newcroft Primary Academy
# Acceptable Use Policy for Primary Pupils


**To keep me safe whenever I use the internet or email, I promise…**

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell an adult I trust if someone asks to meet me offline

**When using computer equipment in school…**

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pIctures of anyone without an adult's permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites at school
- At home I will only use social networking sites for which I am old enough (and with an adult's permission (who knows the age restrictions)
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

**If I break these rules…**

- I understand that the school's behaviour guidelines will be followed

**I have read and understand this policy and agree to follow it.**

Name of pupil _____

Signed _____ Date _____

**I have read and discussed this policy with my child and give permission for him/her to use the school's IT systems, including the internet.**

Parent/Carer signature _____ Date _____