Worksop Priory C of E Primary Academy

e-safety Policy

and

Acceptable Use Agreement

Policy development

The e-safety policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and Safeguarding Children.

- Our policy has been written with full consultation from staff in school and Local Authority advice.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually
- It is available to read or download on our school website or as a hard copy from the school office

Roles and responsibilities
The school has an e-safety team consisting of:

Mr Abbott – Headteacher and Designated Safeguarding Lead
Mr Cawkill – ICT Manager
Mrs Howard – Pastoral Care

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, information retrieval and evaluation.

- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including cyberbullying or unwanted contact. This will include using the CEOP icon to report abuse.
- Issues such as cyberbullying and e-safety will be built into the curriculum to encourage self-efficacy and resilience. Some children with additional needs may need extra support.

Managing Internet Access

Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e-mails.
- Staff to pupil e-mail communication must not take place, however, communications through the blog comment system is encouraged. This communication is public and will be monitored.
- All 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.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil personal details will be published.
- The ICT Manager has editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified. Group photographs will be encouraged rather than full-face photos of individual children.
- Pupils' full names will be avoided on the website and blogs, especially if associated with a photograph.
- Written permission will be obtained from parents and carers in the annual data collection sheets before any photographs are published on the school website.
- Parents are clearly informed of the school policy on image taking and publishing on the data collection sheets.

Social networking and personal publishing on the school blogs

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and students may need educating in their use.
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The school will work with the County Council group to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the ICT Manager.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept of any inappropriate material being seen by pupils to inform policy and educational interventions.

Managing video conferencing

- Video conferencing will be available only for whole class use.
- Video conferencing will use the educational broadband network to ensure quality of service and security.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand-held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

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' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are given access to school IT systems.
- Parents will be asked to sign and return a consent form.

- At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish whether 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.
- Complaints of misuse by staff will be referred to the headteacher.
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the School's Behaviour Policy.

Community use of the internet

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

Communicating the policy

Pupils

- Appropriate elements of the e-safety policy will be shared with pupils.
- E-safety rules will be posted around school and on the computer trolleys.
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be given a copy of the e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting

Parents

- Parents will be notified of the policy on the school website.

- All parents will be asked to sign the parent/pupil agreement every September.
- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

This e-safety policy was revised by: **C Cawkill / P Abbott**

On (date): **March 2017 and approved by Governors.**

ICT Acceptable Use Agreement (AUA)

Policy statement

The Governing Body recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for ICT to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that, along with these benefits, there are also responsibilities especially for ensuring that children are protected from contact with inappropriate materials.

In addition to their normal access to the school's ICT systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment, e-mail and internet facilities during their own time subject to such use:

1. *not depriving pupils of the use of the equipment and/or*
2. *not interfering with the proper performance of the staff member's duties*

Whilst the school's ICT systems may be used for both work-related and for personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times and must never compromise the high standards of safeguarding expected by all members of the staff.

The use of computer equipment, including laptop computers, which is on loan to staff by the school for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy.

Guidance on the use of school ICT facilities

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken up to, and including, disciplinary action.

Further guidance on the responsible use of ICT facilities are contained in the Council document *"Internet Access Policy for Schools"*.

E-mail and Internet usage

The following uses of the school's ICT system are prohibited and may, in certain circumstances, amount to gross misconduct and could result in dismissal:

1. *to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it*
2. *to gain access to, and/or for the publication and distribution of material promoting racial hatred*
3. *for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation*
4. *for the publication and/or distribution of libellous statements or material which defames or degrades others*
5. *for the publication and distribution of personal data without either consent or justification*

6. *where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination*
7. *to participate in on-line gambling*
8. *where the use infringes copyright law*
9. *to gain unauthorised access to internal or external computer systems (commonly known as hacking)*
10. *to enable or assist others to breach the Governors' expectations as set out in this policy*

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

1. *for participation in "chain" e-mail correspondence*
2. *in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives)*
3. *to access ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.*

Use of School ICT Equipment

Users of school ICT equipment:

1. *must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries*
2. *must report any known breach of password confidentiality to the Headteacher or ICT Manager as soon as possible*
3. *must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems*
4. *must not install software on the school's ICT systems, including freeware and shareware, unless authorised by the school's ICT Manager*
5. *must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures*

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

Policy disclaimer

As a member of the Priory School Community, and as someone who has direct or indirect access to ICT equipment, I confirm that I have read the 'E-Safety Policy & ICT Acceptable Usage Agreement (AUA)' and agree to uphold the following additional key points:

- School ICT equipment can be used at home for personal use providing this is under the same regulations as at school
- Staff are not to have 'friends' or 'followers' who are parents of children in the school unless there is a family connection or other specific reason known to the Headteacher on social networking sites such as Facebook and Twitter
- Befriending past (U18 years old) or present pupils is inappropriate on social networking sites such as Facebook and Twitter
- When using social media, personal posts must make no direct or indirect reference to Priory, or any other school that portrays it in a negative way or may bring it into disrepute
- The use of defamatory, abusive or racist language is totally inappropriate, whether directly made by yourself or re-posted/liked/re-tweeted

Where the above regulations are found not to be upheld, this will be treated as a disciplinary matter under gross misconduct. This could ultimately lead to dismissal.

Priory E-Safety and ICT Acceptable Use Policy Agreement

Policy disclaimer

As a member of the Priory School Community, and as someone who has direct or indirect access to ICT equipment, I confirm that I have read the 'E-Safety Policy & ICT Acceptable Usage Agreement (AUA)' and agree to uphold the following additional key points:

- **School ICT equipment can be used at home for personal use providing this is under the same regulations as at school**
- **Staff are not to have 'friends' or 'followers' who are parents of children in the school unless there is a family connection or other specific reason known to the Headteacher on social networking sites such as Facebook and Twitter**
- **Befriending past (under 18 years old) or present pupils is inappropriate on social networking sites such as Facebook and Twitter**
- **When using social media, personal posts must make no direct or indirect reference to Worksop Priory C of E Primary Academy, or any other school, that portrays it in a negative way or may bring it into disrepute**
- **The use of defamatory, abusive or racist language is totally inappropriate, whether directly made by yourself or re-posted/liked/re-tweeted**

Where the above regulations are found not to be upheld, this will be treated as a disciplinary matter under gross misconduct. This could ultimately lead to dismissal.

Signed _____ Date _____