YORKMEAD JUNIOR AND INFANT SCHOOL

e-Safety Policy

Yorkmead school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff and volunteers to share this commitment.

Our Vision

Yorkmead School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and danger. To that end, Yorkmead School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Related Documents:

Acceptable Use Policy for Adults

Acceptable Use Policy for Young People

Data Security Policy

Behaviour Policy

Anti-bullying Policy

Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (Linked from https://www.**birmingham**.gov.uk/.../id/4057/**internet_use_policy**.pdf)

AUP's in context: Establishing safe and responsible behaviours

Policy Owner (DSL and e-Safety Co-ordinator):

Date: September 2017

Review Date: September 2018

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at www.yorkmead.co.uk
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information at parents evenings, information meetings and through the school newsletter

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety co-ordinator has been allocated to Mr Stephen Sutton. He is the central point of contact for all e-Safety issues and will be responsible for day to day

management. All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety co-ordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network
- Be aware that in certain circumstances where unacceptable use is suspected, the person responsible will be accountable for their actions and disciplinary procedures may be instigated.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in an e-Safety log for audit purposes
- Requests for changes to the filtering will be directed to the e-Safety co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the e-Safety log for audit purposes

- The school uses Imperio on all school owned equipment, except mobile devices including laptops, to ensure compliance with the Acceptable Use Policies.

  Pupils use is monitored by Matthew Whitaker and Alex Newman-Smith

  Staff use is monitored by the Head, Alex Newman-Smith and Matthew Whitaker.

- All staff are issued with their own username and password for network access. Supply teachers are given a 'supply' username and password.

Mobile / emerging technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network
- Staff know that they should use their own mobile phones sensibly and that they should not be used during lesson time.
- Pupils should not bring mobile phones to school
- The Education and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Picture/videos of staff and pupils should not be taken on personal devices
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

The school e-mail system is provided, filtered and monitored by Link2ICT and is governed by Birmingham City Council E-mail Use Policy.

- All staff are given a school e-mail address and understand that this must be used for all professional communication
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate e-mails must be reported to the e-Safety co-ordinator as soon as possible.

Published content

The Head takes responsibility for content published to the school web site but delegates general editorial responsibility to Matthew Whitaker. Class teachers and Key Stage co-ordinators are responsible for the editorial control of work published by their students

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution
- The school encourages the use of e-mail to contact the school via the school office/generic e-mail /staff e-mail addresses
- The school does not publish any contact details for the pupils

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in line with DfE guidance and not identify any individual pupil
- Students' full names will not be published outside the school environment

Social Networking and online communication

The school does not allow access to:

Facebook, Twitter, Bebo, MSN and Myspace

Guidance is provided to the school community on how to use these sites safely and appropriately. This includes

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

Un-moderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites.

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Policies before any activity
- Staff and students will be expected to reference all third party resources that are used.

E-Safety Training

The school will undertake a baseline assessment of current staff skills and provide a program of continuing professional development that includes whole school inset, in school support, consultancy and course attendance.

- Educational resources are reviewed by subject co-ordinators and disseminated through curriculum meetings / staff meetings / training sessions
- Pupils are taught how to validate the accuracy of information found on the internet
- Parent sessions are available to provide appropriate advice and guidance. Appropriate advice to parents is provided on the website.

Pupils

- Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the school for this purpose.

- **Parents**

- Parents who help in the school as volunteers are covered by the previous point. Parents who are not voluntary helpers in the school are nonetheless subject
- to the law in the event of misuse of information and communication technology.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998

Data is stored on the school systems and transferred in accordance with the Data Protection Act 1998.

Staff MUST ensure that they do not leave laptops logged on when unattended in order to prevent a 3rd party gaining access to confidential material.

Equal Opportunities

At our school, we teach ICT to all children, whatever their ability and individual needs. ICT forms part of the school curriculum policy to provide a broad and balanced education to all children. Through our ICT teaching, we provide learning opportunities that enable all pupils to make good progress. We strive to meet the needs of those pupils with special educational needs, those with disabilities, those with special gifts and talents, and those learning English as an additional language, and we take all reasonable steps to achieve this.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- Breaches of this policy by staff will be investigated by the headteacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff will be carried out by a least 2 senior members of staff and the Network Manager.
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection

representative and action taken inline with school anti-bullying and child protection policies. There may be occasions when the police must be involved.

- Serious breaches of this policy by students will be treated as any other serious breach of conduct inline with school Behaviour Policy. The system is monitored by Policy Central and any inappropriate use is identified by the Network manager and/or a senior member of staff. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- There is a weekly meeting setup between the ICT Network Manager and the Deputy Head to discuss any breaches of the policy or trends that have been identified.

- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

This policy will be reviewed in **September 2018**.

Signed_____ Chair of Governors

Date:_____