Woodthorpe J.I. School

E. Safety Policy

Our Vision

Woodthorpe J.I. 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 dangers. To that end, Woodthorpe J.I. 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 e-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 of Social Digital Technology and the Internet Policy (AUP) for Adults

Acceptable Use of Social Digital Technology and the Internet Policy (AUP) for Children

GDPR Data Protection Policy

Behaviour/Anti-bullying Policy

Safeguarding/ Child Protection Policy

Social Media and Code of Conduct Policy

Password Security Policy

Publicising E-Safety

To communicate the E-Safety Policy we will:

- Make this policy, and related documents, available on the school website at: http://www.woodthorpe-school.com
- 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 and through the school newsletter and Twitter account.
- Offer annual parental workshops to help disseminate information to our stakeholders.

Roles and Responsibilities

The Headteacher and Governors have ultimate responsibility for establishing safe practice and managing E-Safety issues at our school. There is an E-Safety co-ordinator who is part of the E-Safety Committee who are responsible for policy review, risk assessment, and E-Safety in the curriculum. The co-ordinator is the central point of contact for all E-Safety issues and will be responsible for day to day management. The current members are: Headteacher; Deputy Headteacher/ ICT co-ordinator, Assistant Head Teacher/ SENDCo and Office Administrator.

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

- Follow the E-Safety policy
- Use technology responsibly as stated in the Acceptable Use of School Digital Technology and the Internet Policy for Adults.
- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any incidents to the Headteacher, DSL or E-Safety coordinator 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, enhanced monitoring and procedures may come into action.
- Check that any computer they are using has the latest relevant antivirus installed before accessing the internet/emails.

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 Bishop Challoner. 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 Bishop Challoner to be blocked. All incidents will be recorded in the 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 Bishop Challoner or liaise with the Head teacher as appropriate. The Head teacher controls access to inappropriate sites. Change requests will be recorded in the E-Safety log for audit purposes
- The school uses Policy Central Enterprise on all school owned desktops / laptops to ensure compliance with the Acceptable Use Policies.

We use the Link2ICT monitoring service to provide us with monitoring reports which as well as listing the severity of ‘captures’ identifies patterns that may suggest safeguarding issues. The Headteacher receives weekly reports re this.

Our school iPads have Policy Central Future Digital browser installed on them.

- All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office
- ALL pupils have their own username and a password and understand that this must not be shared

Mobile / emerging technologies

- Teaching staff at the school are provided with a laptop and/ an iPad for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.

- A school mobile phone is issued to staff who may be contacted by pupils or parents e.g. for after school events.
- To ensure the security of the school systems, personal equipment is screened as it is connected to the school network, by the latest relevant anti- virus scan and Policy Central.
- Staff understand that they should use their own mobile phones in accordance with school policy.
- Pupils must sign in phones and gaming devices into the office as they enter school premises in accordance with the Care and Confiscation policy.
- Pupils must not use their mobile phones or other devices, in or out of school, to bully others.
- Pictures / videos of staff and pupils during school time or on school related activities must not be taken on personal devices.
- New technologies are evaluated for their educational benefits and risk assessed, by the ICT Co-ordinator, before they are introduced to the school community.

E-mail

The school uses the Microsoft Office 365 email system, maintained by Bishop Challoner Catholic College.

- All staff and governors are given a school e-mail address and understand that this must be used for all professional communication
- ~~Key stage one pupils have access to class based e-mail accounts that are monitored by the class teacher~~
- ~~Key stage two pupils are given a personal school e-mail address that can be used for class based activities~~
- Staff understand 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 and pupils are not allowed to access personal e-mail accounts on the school system.
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / E-Safety Co-ordinator as soon as possible.

Published content

The Head takes responsibility for content published to the school website. The Leadership Team (LT) and teachers are responsible for the editorial control of work published by themselves and 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 enquiry@woodthorpe-school.com.
- The school does not publish any contact details for the pupils or staff.
- The school encourages appropriate, educational use of other Internet sites and where possible embeds these in the school web site or creates a school account on the site e.g. My Maths
- Class blog sites / Twitter account

Digital Media

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

- Photographs will be published in line with our policy for 'Use of Images of Children' and not identify any individual pupil.
- Students' full names will not be published inside or outside the school environment
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Students understand that they must have their teachers permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the pupils

Social Networking and online communication

Unmoderated 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.

The school constantly reviews the use of social networking sites and online communication and currently does not allow access to any social networking sites.

Guidance is provided to the school community, via links on the website, newsletter, Twitter and parent workshops, on how to use these sites safely and appropriately in the wider world. This includes

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

School App

The school uses an application provided by Schoolzine as our primary platform for communication. This is where all of our digital content is housed. We use this platform to communicate with out stakeholders through the medium of email and notifications.

Educational Use

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 Polices before any activity

- Teachers will check the suitability of sites before using them on the interactive whiteboard. (e.g. YouTube)
- Staff and students will be expected to reference all third party resources that are used

E-Safety training

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

- There is an induction process and mentor scheme available for new members of staff.
- Educational resources are reviewed by curriculum co-ordinators and disseminated through curriculum meetings / staff meetings / training sessions
- E-Safety is embedded throughout the school curriculum and visited by each year group every half term.
- Pupils are taught how to validate the accuracy of information found on the internet
- We recommend parents apply their own age appropriate controls at home. We provide information and guidance on this for parents/carers.
- Training provided by CEOP trained staff at Bishop Challoner.
- Magazines sent home to all parents / carers at least once a year.
- E-Safety help and guidance is embedded within the school's weekly newsletter.

Data Security / Data Protection

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

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and passwords that will be recorded in the school office, and only have access to appropriate content.

Students/ volunteers can only access a limited amount of content in a designated student area on the school system.

Equal Opportunities

We will take all reasonable measures to ensure that all children have suitable access to ICT.

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 and Safeguarding policies.

- Any suspected illegal activity will be reported directly to the police. The relevant provider's service desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Breaches of this policy by staff will be investigated by the Head Teacher. 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 use will be carried out by at least two senior members of staff.

- Breaches of policy will be dealt with by reference to the E-Safety Incident System Grid and recorded on the E-Safety Incident Log, available on the school system. The completed records will be saved securely on the school's intranet.
- Student policy breaches relating to cyber bullying, must be reported to a member of SLT and if necessary to the nominated child protection representative and action taken in line with the school Behaviour/Anti-bullying and Safeguarding Policy. There may be occasions when the police must be involved.
- Although Cyber bullying outside of school is not the direct responsibility of the school, if incidents are reported to school, we will deal with these in accordance with our Behaviour/Anti-Bullying policy and will discipline pupils (see Incidents outside School in the Behaviour/Anti-Bullying policy). We will contact the parents/carers concerned and the police if we think a crime has been committed. We are responsible for educating our pupils in how to keep themselves safe both in school and outside the school environment. This includes E-Safety.
- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour/Anti-bullying Policy and the Breaches of E-Safety Sanctions Grids.
- Minor pupil 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 and the Breaches of E-Safety Sanctions Grids.
- The Educations and Inspections Act 2006 grants the Head Teacher 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.

Sexting

All staff will respond to incidents of sexting, using our procedures which are updated according to the latest advice from Birmingham Safeguarding Children Partnership.

The Rights of Every Child

Woodthorpe JI School uses the U.N. Convention of the Rights of the Child to ensure that every policy supports the improvement of life chances for children. Related articles: 1, 2, 3, 4, 5, 17 and 19.

Signed: 

Approved: 5th June 2019

Review: June 2020