E-Safety Policy

This e-Safety Policy has been put together using guidance from the Worcestershire Local Authority (LA) and is based on the guidance provided by Becta.

OUR VISION

Witton Middle 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, Witton Middle 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.

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: http://www.witton.worcs.sch.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.
- Children must accept the AUP each time they log onto the school system. They also have a copy in their planners which they and their parents sign at the start of each year.
- E-safety is planned into ICT units at all possible opportunities and teachers are also encouraged to respond to anything that arises in their class or year group.
- Provide e-Safety through the school newsletter.

ROLES AND RESPONSIBILITIES

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 the Curriculum Leader for ICT with support from the Senior Designated Person for Safeguarding who is also a member of the senior management team. They are the central points of contact for all e-Safety issues who are responsible for day to day management.

The school has a number of key positions which relate to e-Safety, that are responsible for policy review, risk assessment, and e-safety in the curriculum (see Appendix 1 for e-Safety Team).

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; and
- be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

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, this is the responsibility f the Network Manager.
- Central filtering is provided and managed by Capita IBS Schools. All staff and students understand that if an inappropriate site is discovered it must be reported to the Network Manager who will report it to the Capita IBS Schools Service Desk 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 Network Manager in the first instance who will forward these on to Capita IBS Schools or liaise with the e-Safety team as appropriate. Change requests will be recorded in the e-Safety log for audit purposes.
- The school uses Policy Central Enterprise on all curriculum equipment to ensure compliance with the Acceptable Use Policies.
- Pupils' use is monitored by the Curriculum Co-ordinator and the ICT Network Manager through the report pack with Policy Central.
- Staff use is monitored by Network Manager, who will liaise with the e-Safety team if any issues should arise.
- 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.
- Key stage 2 and 3 pupils have their own username and password and understand that these must not be shared.

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. When staff are issued with school laptops they are expected to sign and act in line with the school's Laptop Policy.

- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network unless approved by the Network Manager.
- Staff understand that they should use their own mobile 'phones sensibly and in line with school policy.
- Pupils understand that their mobile 'phones must be turned off during directed time and kept in the class safes, they are aware of the policy for mobile 'phones in school.
- The Educations and Inspections Act 2006 grants the Headteacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Headteacher will exercise this right at their discretion.
- Pictures/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 Capita IBS Schools and is governed by Worcestershire County 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.
- 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 Network Manager or e-Safety Co-ordinator as soon as possible.

PUBLISHED CONTENT

The Headteacher takes responsibility for content published to the school website but delegates general editorial responsibility to the Business Manager.

- The school will hold the copyright for any material published on the school website 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 addresses/staff e-mail addresses.
- The school does not publish any contact details for the pupils.
- The school encourages appropriate, educational use of other Web 2.0 technologies and where possible embeds these in the school website or creates a school account on the site.

DIGITAL MEDIA

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

- Photographs will be published in line with Becta guidance and not identify any individual pupil.
- Pupils' full names will not be published outside the school environment without permission.
- Written permission will be obtained from parents/carers prior to pupils taking part in external video conferencing.
- Supervision of video conferencing will be appropriate to the age of the pupils.
- Information that might reveal a child's whereabouts are never given.

SOCIAL NETWORKING AND ONLINE COMMUNICATION

The school currently does not allow access to social networking sites and online communication. School staff are expected to behave in line with the Social Networking Policy.

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.

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.

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 websites will be provided instead of open searching for information.
- Pupils will be taught how to conduct safe searches of the internet and this information will be made available to parents/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.
- Staff and students will be expected to reference all third party resources that are used.

E-SAFETY TRAINING

There is a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

- Members of the e-Safety team will liaise with new members of staff and can mentor and support further as required.
- Educational resources are reviewed by the ICT and PHSCE 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.
- Pupils are taught how to validate the accuracy of information found on the internet.
- Pupils are taught how to reference third party resources.

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 Becta Data Security Guidelines. The school follows guidance from the LA on Data Security and follows their recommendations and guidelines.

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 password that will be recorded in the school office.

RESPONDING TO INCIDENTS

Inappropriate use of the school resources will be dealt with in line with other school policies eg Behaviour, Anti-Bullying and Safeguarding Policies.

- Any suspected illegal activity will be reported directly to the police. The Capita IBS Schools Service Desk will also be informed to ensure that the LA can provide appropriate support for the school.
- Third party complaints, or from parents/carers concerning activity that occurs outside the normal school day, should be referred directly to the Headteacher.
- Breaches of this policy by staff will be investigated by the Headteacher. Action will be taken under Worcestershire County 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.
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with

school anti-bullying and child protection policies. There may be occasions when the police must be involved.

- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct inline with school Behaviour Policy. 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.
- Minor student offences, 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 Headteacher 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.

ACKNOWLEDGEMENTS

Birmingham City Council

WMnet

Becta

SWGFL

E-SAFETY TEAM

Mrs. Cath Crossley, Behaviour and Safeguarding

Mr. Matthew Gardner, ICT Network Manager

Mrs. Barbara Humber, Governor with responsibility for e-safety

ASSOCIATED POLICIES

Acceptable Use Policy (AUP) for Adults
Acceptable Use Policy for Young People
Data Security Policy
Behaviour Policy
Anti-bullying Policy
Mobile / emerging technologies Policy
Social Networking Policy
Acceptable Use Policy for Laptops

This policy appears on the school website.

Prepared by:	ICT Co-ordinator	Responsibility of:	ICT Co-ordinator
Agreement Date:	December 2016	Review Date:	December 2018

This Policy was prepared giving due regard to the disabilities and/or special education needs, age, race, religion or belief, sex/sexual orientation, gender/gender reassignment, marriage and civil partnership, pregnancy and maternity of the children and staff at Witton Middle School and its community.

VERSION CONTROL

Date	Version	Approved by	Title	Changes
12.12.16	1	Full Governors	e-Safety	School responsibilities updated
25.09.17	2	Full Governors	e-Safety	School responsibilities updated