Digital Safety Policy

Next review: March 2023

Policy history:

March 2021	Policy updated – reference to Be Internet Legends curriculum included, preventative measures updated	James Bancroft (Principal)
September 2019	Policy updated	James Bancroft (Principal)
March 2018	Policy updated	James Bancroft (Principal)

This policy was reviewed by the Local Advisory Board in the Term 5 meeting, 2020 to 2021

DIGITAL SAFETY POLICY

Purpose

The purpose of this policy is to explain roles and responsibilities in promoting digital safety in school, describe the measures the school will take to safeguarding children and other ICT users and the good practice required to keep our systems secure.

Scope

This policy applies to all members of the school community who have access to and are users of ICT systems, both in and out of the building.

Both this policy and the Acceptable Use Policy relate to the use of any school-owned device used in or out of school, and use of the school's internet.
Deliberate breach of our digital safety policy by pupils may be managed using the school's Behaviour Policy and for staff members this could fall under disciplinary policies. Any form of bullying will not be tolerated and will be handled under the Anti-Bullying Policy.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents/carers of incidents of inappropriate e-safety behaviour.

Safeguarding concerns will be handled under our Child Protection and Safeguarding Children Policy.

Curriculum

At Wistaston Church Lane Academy we understand the responsibility to educate our pupils on Digital Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

We also believe it is important to educate our parents and carers about safe use of technology.

Related Policies

- Acceptable Use
- Safeguarding & Child Protection
- Behaviour
- Staff Disciplinary
- Whistleblowing
- Anti-Bullying
- GDPR (Data Protection)
- Mobile Phone
- Social Media

Roles and Responsibilities

As digital safety is an important aspect of strategic leadership within the school, the principal and LAB members have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named Digital Safety Officer in our school is James Bancroft.

Local Advisory Board

Local Advisory Board members are responsible for:

- Reviewing this policy at least every two years and in response to online safety incidents
- Ensuring the effectiveness of the policy by reviewing how online safety incidents are handled and considering how effective the policy was in managing these incidents
- Receiving regular updates from the Principal in regards to training, identified risks and incidents

Principal

The Principal has overall responsibility for digital safety. The Principal is responsible for:

- Ensuring that digital safety training is planned for staff members
- Ensuring that all digital safety incidents are dealt with promptly and appropriately
- Keeping a log of digital safety incidents

Leadership Team

- All members of the Leadership Team lead the response to behaviour incidents in relation to digital safety.
- Advising the Principal of all relevant digital safety matters

Safeguarding Team

All members of the Safeguarding Team lead the response to any safeguarding incident in relation to digital safety.

- Keeping up-to-date with the latest risk to children whilst using technology
- Advising the Principal of all relevant digital safety matters

They are aware of the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

The ICT Technician (Red Top IT)

The ICT Technician is responsible for ensuring:

- That the school's ICT infrastructure is secure. This will include at a minimum:
    - Antivirus is fit for purpose, up-to-date and applied to all capable devices
    - Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate
    - Internet filtering system is operating correctly

- That passwords are forced to change regularly and that strong passwords are required

The Computing Subject Leader

The Computing Subject Leader is responsible for ensuring:

- The curriculum teaches digital safety appropriately

All Staff members

Staff members must ensure that they:

- Have read and understood this policy
- Have an up-to-date awareness of online safety matters and the current school policy and practices
- Have read, understood, signed and abide by the Acceptable Use Policy
- Ensure that all digital communication with pupils and parents/carers is on a professional level
- Embed digital safety learning in the Computing curriculum
- Respond appropriately to digital safety concerns about children, including those that happen at home
- Consider the importance of data protection
- Report digital safety incidents using CPOMS

Pupils

Pupils of all ages should:

- Participate fully in Computing and PSHE lessons so that they know how to keep themselves safe
- Follow rules set by parents/carers at home
- Tell an adult in school or at home if something upsets them when online
- Pupils are encouraged to inform their teacher or other adults in the school regarding anything which makes them feel uncomfortable while using ICT.

Parents/Carers

Parents and carers will be responsible for:

- Agreeing to the Acceptable Use Policy on behalf of their child
- Supporting the school in managing behaviour incidents when children are using technology both in school and at home
- Making themselves familiar with how to keep their child safe through reading newsletters, using the website and attending digital safety evenings when offered.

Digital Safety Curriculum (part of the Computing Curriculum)

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's digital safety provision. Children need the help and support of the school to recognize and avoid digital safety risks and build their resilience.
Digital safety should be a focus in all areas of the curriculum and all staff should reinforce digital safety messages across the curriculum. The digital safety curriculum should be broad, relevant and provide progression.

We have five internet safety pillars:

- Think before you share (Be internet SHARP)
- Check it's for real (Be internet ALERT)
- Protect your stuff (Be internet SECURE)
- Respect each other (Be internet KIND)
- When in doubt, discuss (Be internet BRAVE)

These pillars are taught using the Be Internet Legends scheme of work (written by Google and Parent Zone): https://beinternetlegends.withgoogle.com/en_uk. In Reception and Key Stage One these safety pillars are discussed with the children frequently. Specific lesson plans are in place for Key Stage Two: https://beinternetlegends.withgoogle.com/en_uk/toolkit.

Embedding Digital Safety Messages across the school

- We try to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- E-Safety rules are displayed in the Computer Areas.
- Pupils will be informed that Internet use will be monitored.
- All staff will be given the Digital Safety Policy and its importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user on any school device at school and off the premises. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the Digital Safety Policy and digital safety messages in newsletters and on the website.

Continuing Professional Development

Training will be offered as follows:

- All new staff should receive digital safety training as part of their induction programme, ensuring that they fully understand the e-safety policy and Acceptable Use Policies
- Staff members will receive regular updates through training sessions and by reviewing guidance documents.
- This Digital Safety policy and its updates will be presented to staff.

We will try to prevent digital safety incidents in school by making technology secure

We use a range of devices. The school will be responsible for ensuring that the school network is as safe and secure as reasonably possible and that policies and procedures within this policy are implemented. 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 aschool computer. However, in order to safeguard pupils and staff and in order to prevent loss of personal data, we do the following:

Security

- Our ICT Technician will ensure that our systems are managed in ways that ensure that the school meets recommended technical requirements
- The ICT Technician will regularly review and audit the safety and security of technology systems
- The LAB will review the findings of the ICT technician's audit
- All users will have clearly defined access rights to school technology systems and devices
- Servers, wireless systems and cabling are securely located and physical access restricted
- Year group logins are used for children in the school as this is age appropriate. The school is aware of the risk associated with not being able to identify individuals who may infringe rules set out in the policy and the Acceptable Use Policy. To address this, pupils should always be supervised and members of staff should not use a pupil login for their own use.
- Guest logins and guest wifi access will be used as appropriate
- Trainee Teachers, supply teachers and visitors will be given the 'guest' login to use and they must sign the Acceptable Use Policy before using the school systems
- Records of administrator logins are stored by the ICT Technician.

Licences and Subscriptions

- Licences will be purchased annually by the School Business Manager
- Software subscriptions will be reviewed annually

Internet Filtering

- We use an educational filtering system that prevents unauthorized access to illegal websites. Illegal content is filtered by the broadband provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and monitored. Access to inappropriate websites is blocked. Access will be reviewed in line with digital safety incidents by the ICT technician and Principal.

Email

- Email accounts are able to detect emails that contain viruses and those that are spam emails.
- All staff members are reminded that their emails are subject to Subject Access Requests, Freedom of Information Requests and during investigations. Email is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Use of personal emails for work purposes is not permitted.

Encryption

- All school devices that hold personal data are encrypted. No data should be stored on un-encrypted devices, e.g. memory sticks. Loss or theft of devices should be brought to the attention of the Principal and this will be reported to the Trust.

Passwords

- Staff members should use strong passwords which are changed frequently.

Antivirus Software

- All capable devices will have antivirus software. This will be updated weekly for new virus definitions. The ICT technician will be responsible for updating this.

Acceptable Use

- Staff members agree to the acceptable use policy at least annually.

- Internet use will be granted to staff when they have signed the Acceptable Use Policy and to pupils (or their parents) after signing the policy.
- When staff members are given devices to use, a loan contract is signed

Managing Emerging Technologies

Emerging technologies will be examined by Computing Subject Leader for educational benefit and a risk assessment will be carried out before use in the school is allowed.