Castle Bromwich Junior School

Where together we can learn, work and succeed.

Computing and E-Safety Policy

Date – March 2026

Reviewed by – Tristi Timms

Review date – March 2027

At CBJS we aim to teach the children to do the best they can, so that they learn the most they can, and develop academically, socially and physically to be as happy and as healthy as they can.

Computing is enriching and dynamic – it prepares children for careers of the future.

1. Introduction and Rationale

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.2 The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

1.3 The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The development and implementation of such a strategy involves all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

1.4 The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

1.5 However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement
- Illegal downloading of music or video files

  The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of the Policy

2.1 This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

2.2 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 school, but is linked to membership of the school.

2.3 The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. Education – pupils

3.1 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

3.2 E-Safety education will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/pastoral
- activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and are guided to validate the accuracy of information

- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- SMART Rules for use of ICT systems / Internet will be posted in all classrooms
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

4. Technical – infrastructure / equipment, filtering and monitoring

4.1 The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password

4.2 Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

4.3 Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

5. Curriculum

5.1 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information

6. Implementation

6.1 At CBJS, computing will be taught both as a discrete subject, and in a cross-curricular way when the opportunity presents itself.

6.2 The mobile computer banks and the PCs distributed around the school will be used to help pupils access the Computing curriculum, along with a range of other resources such as programmable toys.

6.3 The Computing subject leader, ICT Manager and the Headteacher will continually monitor the resources required to deliver the Computing element of the new National Curriculum.

7. Health and Safety

7.1 All users should avoid continuous focus on the screen.

7.2 All users should handle and use equipment with care.

7.3 All users should report any hardware malfunctions to the ICT Manager.

8. Assessment

8.1 Assessment of children's work in Computing is ongoing. Achievement is reported to parents at the end of each academic year.

8.2 Children's work is saved to the server for reference throughout the year. Teachers create portfolios of evidence to show the work completed.

9. Review

9.1 The Headteacher and staff will review this policy in accordance with the development priorities stated in the School's Development Plan. Any suggested amendments will be presented to the governing body for discussion.

10. Use of digital and video images - Photographic, Video

10.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

10.2 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with GDPR with regards the use of such images
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers

10.3 When using communication technologies, the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, DOJO IM etc) must be professional in tone and content
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

11. Data protection

11.1 Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

12. Unsuitable / inappropriate activities

12.1 Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyberbullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

12.2 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

child sexual abuse images
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
adult material that potentially breaches the Obscene Publications Act in the UK
criminally racist material in UK
pornography
promotion of any kind of discrimination
promotion of racial or religious hatred
threatening behaviour, including promotion of physical violence or mental harm
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

using school systems to run a private business
uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
creating or propagating computer viruses or other harmful files   carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
on-line gambling
on-line shopping / commerce
file sharing
use of social networking sites
use of video broadcasting eg Youtube

Appendix A

Internet Safety and the use of Social Media – Year 5 & 6

Dear Parent/Carer

Internet safety and the use of Social Media – Year 5 and 6

Castle Bromwich Junior School is committed to promoting the safe and responsible use of the internet and as such we feel it is our responsibility to raise this particular issue, due to the increase in inappropriate use of Snapchat, Instagram, Facebook and group games such as Fortnight. Many of the issues that have been brought to our attention recently have involved the use of:

- **TikTok** and **YouTube** – online video sharing platforms where people can view and comment.
- **Snapchat** - a photo and video sharing app allowing images and texts to be sent and automatically deleted after a set amount of time. You are required to be at least 13 years old before you can create an account
- **Instagram** - an online mobile photo sharing, video sharing and social networking service which enables its users to take pictures and videos and share them on a variety of social networking platforms. You are required to be at least 13 years old before you can create an account
- **Facebook** - a social networking site. You are required to be at least 13 years old before you can create an account
- **WhatsApp** – An instant messaging app for smartphones. The user agreement requires users to be age 16 or older. Children are often creating 'groups' to which others are joining. This means that all information is shared with anyone who is in the group so privacy is lost and in some cases strangers have been added to the group
- **Fortnight** - a group game where children can be muted and excluded from groups. The recommended age for this game is 13 years

We understand that it is increasingly difficult to keep up with the ways that our children are using new and ever-changing technologies. Our children are immersed in a society that has become dependent on powerful computers, including smart phones, iPads, interactive online games and virtual communities.

Websites such as Facebook, Instagram and WhatsApp to name but a few, offer fantastic opportunities for communication and social connections, however they are created with their audience in mind especially sites such as Facebook and Instagram which are specifically for those over 13 years old. When monitoring your son/daughter's internet use, please remind yourself of the concerns of social media:

- Many sites use 'targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated when they registered. They may have lied about their age to get an account, making them appear older than they are, increasing this risk.

- Young people may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour. The general rule is, if they aren't friends in real life, they shouldn't be 'friends' online
- Language, games, groups and content posted or shared on social media is NOT moderated, and therefore can be offensive, illegal or unsuitable for young people
- Photographs shared by users are NOT moderated and therefore young people could be exposed to inappropriate images or even post their own
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and options • Social media sites can be exploited by bullies and for inappropriate contact
- Social media sites cannot and do not verify its members, therefore, it is important to remember that if your son/daughter can lie about who they are online, so can anyone else

Primarily, these occurrences and reported incidents of misuse of social media sites happen at home, after school hours when children have access to websites that are blocked in school. With this in mind, and in response to concerned parents who have asked for advice regarding internet safety, we feel it important to point out to parents the risks of unregulated use of such sites, so you can make informed decisions as to whether to allow your child to have a profile or not and when and how to monitor their use, particularly at night time. We strongly advise a device free bedroom policy after bedtime to allow for uninterrupted sleep and rest.

Although we cannot govern matters occurring out of school hours which is parental responsibility, we will take action (such as reporting under age profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our pupils, including reporting the use of in appropriate images of young people to the police, as this is a legal matter. This also refers to inappropriate text messages.

Should you decide to allow your child to have an online profile we strongly advise you:

- Check their profile is set to private and that only their friends can see information they post • Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting or messaging offensive /inappropriate messages or photo's
- Monitor your child's use of language and how they communicate to other people, ensuring profanity is discouraged
- Have a look at advice for parents on the social media sites
- Set up your own profiles so you understand how the site works and ask them to have you as their friend on their profile so you know what they are posting online

Make sure your son/daughter understand the following rules:

- Always keep your profile private
- Never accept friend you do not know in real life

- Never post anything which could reveal your identity including photographs wearing school uniform where possible
- Never post anything you wouldn't want your parents or teachers to see
- Never agree to meet somebody you only know online without telling a trusted adult • Always tell someone if you feel threatened or someone upsets you

We recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online:

www.thinkuknow.co.uk www.net-aware.org.uk www.getsafeonline.org

Through lessons provided at school, assemblies, guest speakers, and PSHE lessons, we do our best to provide our children with the awareness and knowledge they need in order to recognise and avoid dangerous, destructive, or unlawful behaviour and to respond appropriately. However, it is only through a collaborative effort between parents and teachers that we will succeed in creating responsible and safe cyber citizens.

Yours sincerely,

Mrs Timms