Belgrave St Bartholomew's Academy

Principal: Mr G. Barlow

Online Safety Core Policy and Audit

If you would like this translated in Urdu, please contact the school office.

آپ اردو ترجمہ میں یہ خط چاہتے ہیں تو، اسکول کے دفتر سے رابطہ کریں.

ONLINE SAFETY POLICY

Introduction

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The policy will operate in conjunction with other policies including those for student Behaviour, Anti-Bullying, Curriculum, Data Protection and Safeguarding.

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

Vision and values

All members of the school contribute to the life of our happy, respectful and successful school. We ensure that our values; courage, compassion and respect are at the heart of all that we do. From the minute you step inside our academy, you will see that we all work towards one main aim; 'Being the best that we can be, together.' Every child and adult is encouraged to flourish and reach their full potential regardless of age, gender, ability or faith and we do this together, as a family. We are passionate about working in partnership with pupils, parents and carers to protect the Belgrave family.

At Belgrave St Bartholomew's Academy we are passionate about ensuring that our learners develop sound knowledge, understanding and skills; to enable them to actively demonstrate effective online safety practices. Curriculum planning will build on pupil's previous learning and is progressive. Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. To prepare children for life we need to ensure they are critical users of technology and the internet- thinking carefully about their choices before clicking and exploring.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Schools Broadband with effective filtering systems.
- National Education Network standards and specifications.

Legislation and Statutory Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping children Safe in Education 2023 and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good

reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. The Keeping children Safe in Education 2023 document sets out the legal duties that must be followed to safeguard and promote the welfare of children and young people under the age of 18 in schools and refers to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Intent

- To ensure that all members of our academy community understand and are committed to promoting respectful and responsible internet use.
- To ensure that staff and pupils are aware of the benefits and risks associated with internet use and the use of social media.
- To ensure that all necessary measures are in place to safeguard all.
- To ensure that pupils feel safe and secure and are aware of how to keep themselves safe online.
- To ensure that all members are aware of their responsibilities to safeguard themselves and others when accessing the internet and engaging in online activities.

Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Curriculum, Bullying and Child Protection.
The school has appointed Online Safety Co-ordinators: **Mr G. Barlow and Miss S. Sardar.**
The Online Safety Policy has been written by the school, building on the Stoke-on-Trent E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors and the PTA.
The Online Safety Policy and its implementation will be reviewed annually.
The Online Safety Policy was revised by: **Mr G. Barlow and Miss S. Sardar.**

It is being submitted to the Local Governing Committee for approval on: *12th December 2023.*

Further Information

Stay safe online- NSPCC E-Safety materials and curriculum E-Safety advice — **0808 800 5000** / www.nspcc.org.uk

ThinkUKnow- E-Safety E-Safety materials For parents/Teachers — https://www.thinkuknow.co.uk/

Police Website for E-Safety issues/reports — https://www.ceop.police.uk/Safety-Centre/

Online Safety Audit – Belgrave St. Bartholomew's Academy

Has the school an Online Safety Policy that complies with C&YP guidance?	Y
Date of latest update: October 2023	

The updated policy will be shared with the Local Governing Committee on: 11th December 2023	
The Policy is available for staff at: Belgrave St Bartholomew's Academy	
And for parents at: Belgrave St Bartholomew's Academy	
The Designated Child Protection Coordinator is: Mr G. Barlow (Principal)	
The Online Safety Coordinator is: Mr G. Barlow (Digital Lead) & Miss S. Sardar	
Has Online Safety training been provided for staff?	Y/N
Has Online Safety training been coherently planned and delivered for pupils? –***ongoing across all year groups and embedded in the Curriculum.***	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the school Online Safety Rules?	Y/N
Have school Online Safety Rules been set with pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access (e.g. Schools Broadband).	Y/N
Is personal data collected, stored and used according to the principles of the General Data Protection Regulation 2018?	Y/N
Do all school computers have Online Safety text monitoring software (Forensic) installed?	Y/N
Has the school filtering policy been approved by SMT? (N/A unless school has taken over responsibility)	Y/N
If the school has taken responsibility for its own web filtering, have appropriate members of staff attended training on the filtering system and are appropriate procedures in place?	Y/N

Implementation

Teaching and learning

In September 2019 the school moved to 1:1 iPad implementation with the children. The iPad is a tool for teaching and learning. Through the use of Apple Classroom, the staff can monitor the individual use of each iPad in their class. Through the app they can also safely navigate and lock children in and out of a variety of apps and websites. Staff are also aware that, if needed, they can lock iPads in order to check history and usage of each individual pupil. The use of Apple Classroom, Apple Manager, Lightspeed and Jamf will further enhance our monitoring and Online Safety procedures.

Keeping children safe using iPads

- Staff are aware that the iPad is a tool to enhance teaching and learning through feedback and creativity.

- Staff understand that too much screen time is not good for the children.
- G.Barlow (Principal)/Bridge (Digital Lead) will manage the iPads using Apple School Manager.
- Internet safety filters applied to all pupil iPads. Children have individual Safari logins to ensure safe use and tracking of inappropriate use.
- Staff trained on use of Apple Classroom which displays a live feed of children's screens to ensure safe use.
- Staff to 'Navigate' and 'Lock' pupil iPads when appropriate.
- If children do misuse the iPad, they will receive a ban (based on severity of incident) and alternative resources to be made available in the classroom.
- Outside agency Apple school support available through Sync and an Apple Specialist teacher (RB).
- If the children are using the iPads at home, parents will need to attend a meeting in school to discuss responsible use of devices.
- Parents will sign a declaration accepting responsibility of use of the iPad when it is at home.

Why are new technologies and Internet use important?

- The internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside of school and will need to learn how to evaluate Internet information and to take responsibility for their own safety and security.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include Internet usage monitoring and web filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities and to raise attainment and achievement. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content.
- The academy will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be Taught How to Stay Safe Online

At Belgrave, we educate our very youngest learners about the importance of online safety as we recognise that pupils are accessing an online world both in the home and school environment.

In Key Stage 1, pupils will be taught to:
• Use technology safely and respectfully, keeping personal information private.
• Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:
• Use technology safely, respectfully and responsibly.
• Recognise acceptable and unacceptable behaviour.
• Identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects where relevant. The academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Cyber-Bullying
The rapid development of and widespread access to technology has provided a new medium for 'virtual bullying', which can occur in and outside school. Cyber-bullying is a different form of bullying which can happen beyond the school day into home and private space, with a potentially bigger audience, and more accessories as people forward on content.
The importance of respectful online communications is explicitly taught and all pupils and parents are aware of our expectations. The school will take all reasonable precautions to ensure against cyber-bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.

- The school will proactively engage with pupils in preventing cyber-bullying by:
    - Understanding and talking about cyber-bullying, e.g. inappropriate use of e-mail, text messages;
    - Keeping existing policies and practices up-to-date with new technologies;
    - Ensuring easy and comfortable procedures for reporting;
    - Promoting the positive use of technology;
    - Evaluating the impact of prevention activities.
    - Pupils, parents, staff and governors will all be made aware of the consequences of cyber-bullying.
    - Parents will be provided with an opportunity to find out more about cyber-bullying through: session for parents, NSPCC support guidance, Know It All parents' and other outside agency support.

How will cyber-bullying reports/issues be handled?
Records of any incidents of cyber-bullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risk will be reviewed regularly.

- Complaints of cyber-bullying will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head of School.

- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyber-bullying.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
    - Interview/counselling by the class teacher;
    - Informing parents or carers;
    - Removal of Internet/computer access for a period of time or banning of mobile phones in school.

Radicalisation and Extremism

Belgrave takes an active role in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. In the same way teachers are vigilant about signs of possible physical or emotional abuse, we are vigilant about any signs of radicalisation or extremism in any of our pupils. We follow the same safeguarding procedure to ensure all children in our care are well looked after. Any suspected cases will also be reported to Mrs L. Jones (Prevent Lead).

Information system security

- Virus protection will be updated regularly on all networked computers. Virus Protection will be updated by ICT Trust Support Team.
- Academy systems continually remind users that school systems are protected by forensic software. Any irregularities are monitored by Mr G. Barlow and Mr S. Robinshaw/Mr M.Latos (Trust Digital Lead), any breach of the academy policies could result in disciplinary actions.

E-mail

(Currently blocked and only opened if teacher requests e.g. covering within the curriculum)

- Pupils may only use approved e-mail accounts/messaging systems on the academy system with express permission and approval from staff.
- Pupils must immediately tell a teacher if they receive offensive e-mail or messages. Pupils must ensure that such emails are not deleted.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters will be actively discouraged and the potential harm that can be caused will be included within Online Safety learning.
- Filtering of email content will be completed as the school has filtering software available.

Web Publishing pupils' images and work

- Images, published to the web, that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Permission will be gained from parents to use pupil's images in line with GDPR regulations.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Pupils' first names can be used.
- Written permission from parents or carers will be obtained before images of pupils are electronically published to the web, with permission to publish first names.

Social networking and personal publishing

- The City Council/school (Lightspeed) will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Newsgroups will be blocked unless a specific use is approved.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils and parents will be advised that the use of social network spaces, outside school based controlled systems is inappropriate for primary aged pupils, unless strictly supervised.
- Staff and pupils should be advised not to publish specific and detailed private thoughts on social networking sites.

Public Web published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published on the school website.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The Principal and staff will take overall editorial responsibility of the website and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

Filtering and Monitoring

- The school will work in partnership with Lightspeed to protect children and staff in school through effective filtering and monitoring in line with DFE expectations and KCSIE.
- Lightspeed is the system used to alert the Senior Leadership Team (SLT) when a child has searched for an inappropriate term or has tried to access a filtered website. Lightspeed identifies the device used and therefore the child (as each device is allocated to an individual pupil, not shared). The following process is followed when a filtering and monitoring incident occurs:
- SLT will inform the class teacher of the incident (from the Lightspeed notification).
- Class teacher investigates and has a restorative conversation.
- Class teacher issue an appropriate consequence (for example S4 logged on Arbor 'Inappropriate Use of iPad')
- Class teacher inform parents.
- Class teacher log on CPOMS using 'Filtering and Monitoring' category.
- SLT also keep log of all incidents to identify patterns and trends and will act for repeat offenders.
- Jamf will now be used to update and manage individual iPad devices. ICT technician (SR) leads this, but access is available for Digital Lead/Apple Learning Specialist (Mr G. Barlow).
- The MDM for iPad devices is Apple Manager and access is available for ICT Technician and Digital Lead.
- Any misuse of iPads will firstly be dealt with by the class teacher. If this continues staff will report the misuse to Mr G. Barlow and parents will be informed of their child's conduct.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and protocols will be established before use in school is allowed. (Mr G. Barlow/Mr D. Jones)
- Pupils are not allowed mobile phones in school unless specific permission has been given by the Principal, Staff and visitors must ensure that mobile phones are switched off and secured out of view from pupils.
- We do not use mobile phones to record images of pupils or access/comment on social media during school time.

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 and the school complies with the General Data Protection Regulation 2018 requirements.

Managing remote teaching/video-conferencing

The equipment and network

- Full IP videoconferencing will use the national educational or the schools' broadband network to ensure quality of service and security.
- All videoconferencing equipment in the school/classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.

- Videoconferencing contact information will not be put on the school website.
- School videoconferencing equipment will not be taken off school premises without permission, since use over a non-educational network (e.g. the internet) cannot be monitored or controlled.

Users

- Pupils will ask permission from the supervising teacher before making or answering a videoconference call if this is available in the near future.
- Videoconferencing will be supervised appropriately for the pupils' age.
- Parents and guardians will agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Only key administrators will be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.
- When delivering Zoom lessons staff will always team teach in order to monitor safe and appropriate use of technology.

Content

- When recording a videoconference lesson, written permission will be sought by all sites and participants. The reason for the recording is given and the recording of videoconference is clear to all parties at the start of the conference.
- Recorded material will be stored securely.
- If third-party materials are to be included, recordings will be checked that they are acceptable to avoid infringing the third party intellectual property rights.
- Dialogue will be established with other conference participants before taking part in a videoconference. If it is a non-school site it is checked that they are delivering material that is appropriate for the class.

Pupils using devices for home learning

- IPads will be used at home by children to access home learning set by staff.
- Staff will provide feedback on work completed and monitor the safe use of the iPads.
- IPads are managed through Jamf (G. Barlow/ D. Jones) and set to lock at 8pm to reduce screen time and the risk of inappropriate use.
- Agreement signed by parents clearly shows the SMART Online Safety guidelines.
- Home learning policy will follow SBMAT Acceptable Use Policy and Remote Learning.

Policy Decisions

Authorising Internet access

- All staff must read and adhere to the 'SBMAT User Agreement' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

- Parents will be asked to sign and return a consent form.
- Sanctions for inappropriate use will be drawn up and shared with staff and pupils.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor St. Bart's Academy Trust can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly. If unsuitable material appears, the Online Safety Leader & Senior Leaders will be informed so that relevant filtering can be completed.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the class teacher and where necessary a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Mrs J. Craig/ Mr G. Barlow)
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils are expected to work in partnership with staff to resolve issues or concerns.
- Sanctions within the school behaviour policy will include:
    - interview/counselling by ELT/SLT;
    - informing parents or carers;
    - removal or restriction of Internet or computer access for a period.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all networked rooms and discussed with pupils at the start of each year and as the need arises.
- Pupils will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- Online Safety modules will be included in the PSHE and Computing programmes covering both school and home use.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. In addition, all staff members will revisit or review this training as part of our annual safeguarding updates

Enlisting parents' support

- Parents' attention will be drawn to the school's Online Safety Policy in relevant newsletters, prospectus, the school website and through parent workshops.

- A guide to Responsible Internet Use is also available on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Online Safety updates will be shared on both Class Dojo and other school social media to keep parents updated on relevant information.

Mobile Technology Device Policy

All devices that have access to a) the internet and b) the school network must be password protected. The purpose of this is to prevent data loss and protect pupils and staff.

Staff passwords

Staff each have their own username and unique password. Staff generate their own password and understand that they must not share passwords. Records of staff passwords are not stored but the passwords can be overwritten or reset by the network administrator. Staff are expected to change their passwords at least annually to ensure that they remain secure. Staff with access to sensitive data change their passwords every term.

Pupil passwords

Each pupil has their own username and password for use on Spelling Shed, Doodle and other software. Staff monitor the use of iPads in order to track any un-safe behaviour online or misuse of ICT software and equipment.

USB device password

USB devices are encrypted and password protected. The encryption password is universal.

Hard drive encryption password

Laptop hard drives are encrypted and password protected. The encryption password is universal.

Please also refer to SBMAT Acceptable Use Policy; Learners and Staff.

Personal mobile devices – staff and visitors

- Staff and visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff and visitors should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of devices (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Staff and visitors are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.

- Should there be exceptional circumstances (e.g. acutely sick relative), then staff and visitors should make the Principal and office staff aware of this so messages can be relayed promptly.
- Staff and visitors should report any usage of mobile devices that causes them concern to the Co-Principals.
- All staff and visitors must password protect their mobile device

Personal mobile devices - pupils

- Pupils to only have phones when permission is granted from the school and parents in circumstances such as Year 6 children walking home alone.
- Phones must be switched off during the school day.
- Emergency contact to be made through the school office
- Children are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.

School owned mobile devices – staff

- All mobile devices including USB sticks must be password protected to prevent data loss
- All mobile devices must be protected by the school's web filtering system
- Passwords to devices must not be shared with anyone who is not employed by the school
- All staff will sign the Acceptable use policy agreement through Parago

School owned mobile devices - pupils

- All mobile devices must be protected by the school's web filtering system
- Devices intended for pupil use must not leave the school
- Pupils must access mobile devices using pupil user accounts only
- Pupil mobile device user accounts must block any attempted file downloads, block access to the computer's system files, block access to the control panel, block access to the command prompt and only map the student network drive.

Miscellaneous

- SSID access code to be held by the ICT technicians, Co-Principals and Computing Lead only.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key Online Safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Networked favourites Ikeepbookmarks.com
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Yahooligans CBBC Search Kidsclick Kiddle (Google kids) Safari (log in)
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	School Net Global E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and	Pupil and parental consent should be sought prior to publication.	Making the News Dojo Podcasts

other websites for feedback.	Pupils' full names and other personal information should be omitted. Pupils should be encouraged to report any inappropriate comments.	Video/Film Photograph
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within blogs, chat rooms or online forums.	Only blogs/chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype Zoom FlashMeeting Purple Mash Teams
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Zoom FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum Teams

Belgrave St Bartholomew's Academy - Sanctions for inappropriate use of ICT

In the event of ICT equipment being used inappropriately by pupils in school, relevant steps will be taken by the class teacher. These steps should be as follows:

- If it is not deemed a serious enough incident of inappropriate use, a warning and sufficient punishment will be given by the class teacher in line with the school's behaviour policy, which may result in the step system being used.
- If an incident is deemed sufficiently inappropriate, the relevant piece of ICT equipment will be taken off the child and stored securely for further analysis or evidence gathering. If the matter includes any safeguarding incident, the school safeguarding officer will be informed. A member of the Senior Leadership team will be informed and any relevant evidence will be passed on to them. All information and evidence will be recorded in the class log books. If deemed necessary the appropriate authorities will be informed.
- It is the responsibility of the class teacher to record any Online Safety concerns and report these to the parents (if this is an incident that is occurring at home). Staff to record welfare concerns on CPOMS to inform relevant staff.