Acceptable use of ICT and E-Safeguarding Policy January 2024

Bushmead Primary School

1. Aims

At Bushmead Primary School, we recognise that information and communication technology plays an important part in learning. All stakeholders in school must use technology appropriately, safely and legally. We have a major responsibility to teach children the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

2. Legislation and Guidance

This policy complies with the following legislation and guidance:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Roles and Responsibilities

4.1 The Governing Body

- The school governing body have responsibility for ensuring that the school has an Acceptable use Policy of ICT and e-Safeguarding Policy and this policy is reviewed annually.

4.2 The Head Teacher

- The head teacher is ultimately responsible for e-Safeguarding for all members of the school community, though day to day responsibility for e-Safeguarding may be delegated to the e-Safeguarding coordinator.
- The head teacher must ensure that there is a designated person for coordinating e-Safeguarding and acceptable use of ICT, this should be a member of the management team and preferably also a designated person for child protection.
- The head teacher is responsible for ensuring that the e-Safeguarding coordinator receives suitable training to enable them to carry out their role

4.3 The e-Safeguarding Coordinator

- To promote awareness and commitment to e-Safeguarding throughout the school
- To be the first point of contact on all e-Safeguarding matters
- To take day to day responsibility for e-Safeguarding within school and have a leading role in establishing and reviewing the school's Acceptable use of ICT and e-Safeguarding Policy and procedures.
- To create and maintain e-Safeguarding policies
- To ensure that all staff are aware of the procedures that need to be followed in event of an e-Safeguarding incident

- The e-Safeguarding coordinator will ensure that all computers have up to date virus protection, monitoring software and an internet connection which is filtered through the regional broadband consortium (ENBN)

- The e-Safeguarding coordinator and technical staff will meet on a regular basis to discuss monitoring and follow up any arising issues.

4.4 All Staff and Volunteers

- All staff have a responsibility to use ICT appropriately and legally and report any illegal or inappropriate use of ICT to the head teacher or the e-Safeguarding coordinator, as soon as possible.

- Teachers and teaching assistants should address issues of e-Safeguarding when using the internet with children

4.5 Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, national or local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- access to parents' sections of the website

5. Access to ICT

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. The ICT equipment is stored securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware and will be kept active and up to date.

All staff users will adhere to The Acceptable Use and e-Safeguarding Policy provided by the school. Users must take responsibility for their use and behaviour while using the school ICT systems and be aware that such activity will be monitored and checked.

At Key Stage 1 and Key Stage 2 pupils will access the internet using a class ID and password, which the class teacher supervises. All internet access will be undertaken with a member of staff within the same room.

6. Use of the Internet

The school encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. Internet usage means any connection to the Internet via Web browsing, use of the learning platform, external email or news groups. The school has an obligation to fulfil its Prevent Duty and to ensure that no extremist or terrorist material can be accessed.

The school expects all users to use the Internet responsibly and strictly according to the following conditions:

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting extremism or terrorism
- promoting illegal acts

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK
- extremist or terrorist material

Sites must not be accessed which contain inappropriate material defined below:

- Personal ads or dating
- Criminal skills or resources
- Internet based peer to peer networks e.g. Pirate Bay
- Downloads of ring-tones, screensavers and games
- Downloads of freeware, shareware or evaluation packages (excepting by authorised persons as designated by the school and in compliance with copyright law)
- Illegal drugs
- Hacking, virus writing or password cracking
- Gambling
- Depiction or avocation of violence or the use of weapons
- Breach of copyrights
- Instant messaging or online chat rooms not directly related to education or educational use.

Prohibited material will include any material which may be construed as offensive on the grounds of gender, race, ethnic origin, disability, sexuality, religion, age, HIV status, size, stature, trade union membership/office or any combination thereof or any group identified under the Equality Act 2012.

If inappropriate material is accessed accidentally, users should immediately report this to the head or designated e-Safeguarding co-ordinator so appropriate action can be taken.

Access to internet web sites that are unrelated to school business should be restricted to out of school hours and designated breaks and should not leave a web history that through which children may access inappropriate content. Where staff are unsure on whether given content is appropriate, they should contact the e-Safeguarding Co-ordinator for clarity.

The use of YouTube as a teaching tool is allowed providing staff have vetted the video prior to the lesson to assess that the content is appropriate. Staff should use the freeze screen function when loading the video in case of any adverts appearing that could contravene this policy.

Conducting Financial Activities on the Internet

While this policy does not ban the use of the internet for conducting personal financial transactions, e.g. e-banking, we warn against it on school machines. Residual information from such activities can be left on the computer hard drive and could subsequently be accessed by others. Similarly, personal or financial information may be inadvertently recorded by the school's monitoring software. The school or the local authority do not accept any liability for any resulting loss or damage.

Intellectual Property, Plagiarism and Copy Right

Any information copied or downloaded from the internet and then re-presented in any form should acknowledge the source. Any images used should be copyright free.

7. Email use

E-mail should never be sent, forwarded or replied to where the content is;

- Abusive
- Bullying
- Defamatory
- Disruptive
- Harmful to the school or local authority
- Harassing
- Insulting
- Intolerant
- Obscene
- Offensive
- Politically biased
- Threatening

Staff Email

Any communication with children via email should be through a school email account (e.g. **mstaff@bushmead.cambs.sch.uk**.)Do not release or in any way make available personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) over through email or the internet.

The sending of email(s) that are wholly or substantially unrelated to school business should be restricted to out of hours and designated breaks and not completed using a school email account.

8. Images of children

Written permission from parents or carers is obtained for the following locations before photographs of pupils are published. This will be done annually at the Autumn Parents Evening and on entry to the school. A record of children with/without permission for images is held in the school office.

- On the school website
- In the school prospectus and other printed promotional material, e.g. newspapers
- In display material that may be used around the school
- In display material that may be used off site
- Parents and carers may withdraw permission, in writing, at any time.

Pupils and staff will only use school equipment to create digital images, video and sound involving children. In particular, digital images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online.

Staff may take digital images of children on a personal device on a residential or sporting trip, where uploading images and tweeting are a means of communicating with parents. Staff should only do this with the Headteachers permission. The date and circumstances will be recorded, and staff will be given the next working day to download all digital images onto the school system and delete them from the personal device.

Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.

When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Any images, videos or sound clips of pupils must be stored on the school system and never transferred to personally-owned equipment. When staff are accessing the remote desktop from personally owned machine, they're prohibited from downloading such material to their own device.

Social Networking

Staff and children are not allowed to use their personal account on social networking sites, such as FaceBook, or Instragram in school or on school machines unless they have been given permission by Senior Leaders. If staff have social networking accounts we recommend that their profiles are set to private. Staff must not have contact with children from our school through social networking sites.

This is part of the Safer Code of Conduct Policy;

8.1 Staff in school should not establish or seek to establish social contact with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship. This includes social networking sites such Facebook, Instagram, Snapchat, and blogging. Even if a pupil seeks to establish social contact,

or if this occurs coincidentally, the member of staff should exercise her/his professional judgment in making a response and be aware that such social contact in person, by phone or on the internet could be misconstrued and may place the member of staff in a very vulnerable position.

8.2 Staff and volunteers must not give their personal details such as home/mobile phone number; home or e-mail address to pupils unless the need to do so is agreed with senior management.

8.3 Where pupils have access to their own school email address, they are free to share their work with their teacher/group leader. The teacher should ensure that responses made are directly related to work shared, in the same manner as when marking a child book or giving verbal feedback. This should always be completed through a school email account ending in: @bushmead.cambs.sch.uk

Staff should not post or make comments on social networking sites that may be interpreted as negative or harmful to the school, its employees, children or the local authority.

E2BN guidance on using Facebook safely, as a school employee, can be found here:
http://www.e2bn.org/files/YHGfL_Guide_to_Using_Facebook_Safely2010.pdf

Face book provides support and advice for 'Educators' using Facebook:
http://www.facebook.com/help/?safety=educators

9. Mobile Phones

Ordinarily, staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Staff must use a school phone where contact with pupils, parents or carers is required.
Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

The recording, taking and sharing of images, video and audio on any device is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher e.g. residential school trips. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. All videos should be removed from the device as soon as possible and disposed of securely at the end of the period of work. Staff devices should use encryption and advanced password where available. (See Point 5)

Where staff members are required to use a mobile phone for school duties, for instance in case of an emergency during off-site activities, they can use their own devices if they 'withhold' their own mobile numbers for confidentiality purposes. This is done by preceding the telephone number with the digits 141 before calling, e.g. 14101733123456. This will prevent the caller's number being displayed on the receiving phone.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox etc.)

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

Pupils should not bring mobile phones or personally-owned devices into school unless they are in Year 5 and 6. These are then stored in a locked box in the classroom. Mobile phones will be returned at the end of the school day. If a pupil brings a mobile phone into school, who is not is Years 5 or 6, the parent will be contacted to collect the phone and it will be retained in the school office for safe keeping. The school takes no responsibility for personally owned devices brought into school.

10. Internet Games

There are times in the week when children have 'free' use of the school network, such as during wet playtimes, reward time for good behaviour etc. However, this access is still supervised by an adult. Any games played on the school network must be in line with the school rules and be suitable for primary aged children.

11. Data Protection

Personal data will be recorded, processed, transferred and made available according to the
The UK General Data Protection Regulation (UK GDPR), which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

12. Downloading Music

Children should not download music onto the school network. If music is free to download it is usually illegal. Staff may download music, but this must be done legally, in line with copyright laws and for use within school e.g. from the Sing-up website and can only be completed by a 'Power User'.

13. Monitoring

The school uses a software package UniFi Network which monitors the wireless use of ICT. This software will;

- Log all computer activity to a central database
- Monitor and record an unlimited number of screens in real-time
- View current and previously opened windows, websites, applications, printed documents and deleted files

Internet use is monitored by the Local Authority and they are responsible for

- Detect written keywords or sentences with screenshot or video evidence
- View evidence of attempts to access banned windows, websites and applications
- Instantly alert you of violations such as attempts to access banned websites

14. Sanctions

Sanctions will be levelled to the seriousness of the offence. For example, temporary suspension of ICT rights for minor offences, ranging to permanent exclusion, disciplinary action and involvement of the police for illegal actions.

15. School website

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. The school obtains parental permission before using images of pupils. We ensure the image file is appropriately named – we do not use pupils' names in image file names or ALT tags (Alt tags are the labels that describe the images on a website) if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. We will use group photos rather than photos of individual children, wherever possible.

16. Facebook

The school promotes news and events through Facebook. Staff given access to post by Senior Leaders should adhere to the following point:

- Ensure posts reflect well on the school.
- Never refer to a political preference
- Do not use the names of pupils where their photo is present
- Check posts carefully before submitting, where possible checking the content with a colleague
- Report any unwelcome comments by visitors to the Head teacher or Deputies

- Ensure photos have been checked against the schools permissions list

17. Curriculum Use of ICT

Filters are set differently for students and teachers to allow appropriate access.

Staff are able to save work through either the staffshare or my documents, which are both redirected to the school network. My documents are held under the individual account.

Teachers should follow the national curriculum for Computing and ICT. When teaching the National Curriculum, teachers should ensure that iPads are used for educational applications (apps) and not for browsing the internet. Where research lessons are conducted on iPads, children should complete this through safe browsers such as Britannica Learning. Where more thorough research is needed, children should log in to a computer/laptop. Children should always be supervised whilst using iPads.

18. Reporting and dealing with incidents

Incidents of concern must be reported to the Headteacher.
Any concern regarding children's safety to the Designated Child Protection Coordinator.
If you find inappropriate or illegal material on a PC or other electronic device in school, do not try to capture or copy evidence, this may leave you in the position of distributing illegal images. Ensure children cannot access the inappropriate or illegal material - turn off the screen, remove the device to a secure place or switch off power at the wall. You then MUST report this to the Headteacher.

19. Monitoring and Review

This policy and information report will be reviewed by the governing body every year. It will also be updated if any changes to the information are made during the year.

It will be approved by the governing board.

20. Related Policies

This policy has links with, and works alongside the school's ICT, child protection and anti-bullying policies.

Version:	4	
Written by:	Ann Coffey	**Date:** 18th January 2024
Last reviewed by staff:	January 2024	
Last reviewed by governors:	Spring 2 2024	
Next review due by:	Spring 2 2025	

Appendix 1:

All Staff Awareness and Responsible Use of ICT and Data Protection Agreement

This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT and are aware of the implications of Data . All staff are expected to sign this agreement and adhere at all times to its content. Any concerns or clarification should be discussed with the PA to Senior Leadership Team.

- I will only use the school's e-mail/Internet/Website and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will comply with Bushmead Primary Schools system security and not disclose any passwords provided to me by the School or any other related authorities.
- I will only use the approved secure email system for any Bushmead Primary School business.
- I will not install any hardware or software without permission from the PA to Senior Leadership Team. Home printers and home internet access are automatically approved.
- Images of pupils will only be taken, stored and used for professional purposes in line with the Bushmead Primary School data protection policy and with written consent of the parent or carer.
- I confirm that, in the event that I notice inappropriate use of social networks, school computers or use of the internet by staff, pupils or parents, I am aware of the correct procedure to escalate these concerns.
- I will ensure my online activity, both personal and when at school, specifically using any social media websites, will not bring my professional role, nor Bushmead Primary School into any disrepute.
- I will support and promote Bushmead Primary School e-safety guidelines.
- I will not place any confidential information, relating to pupils, staff or Bushmead Primary School on memory sticks, unless password protected and encrypted or other such devices.
- I understand that my use of the school Internet and school e-mail can be monitored and logged.
- All data (paper or electronic) relating to pupils, staff and members of the Bushmead Primary School Community will be kept secure in accordance with the UKGDPR Policy.

Signed:

Name:

Date:

Appendix 2

This agreement will be sent annually to all parents and they will be asked to consent using ParentPay

School's Acceptable and E-safety agreement form for parents and carers.

- As the parent or legal guardian (s), I grant permission for my child to have access to use the Internet, school Email and other ICT facilities at school.

- I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use and understand that my son/daughter may be informed if the rules have to be changed during the year.

- I know that the latest copy of the Acceptable Use and E-Safety Policy is available at from the school office or on the school website and that further advice about safe use of the Internet can be found on the school's website.

- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching esafety skills to pupils.

- I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

- I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Consent provided using ParentPay

Appendix 3:

Pupil Acceptable Use and E-safety Agreement

These E-safety Rules help to protect pupils and the school by describing acceptable computer use.

- I understand the school owns the computer network and learning platform and can set rules for its use to keep me safe.
- I will only use ICT systems in school, including the internet, email and digital pictures for school purposes.
- I will only log on with my own user name and password.
- I will not share my passwords with anyone.
- I will only use my school email address at school.
- I will make sure that all messages are responsible, respectful and sensible.
- I will be responsible for my behaviour when using the Internet/learning platform. This includes resources and the language I use.
- I will use the forums on the school's learning platform for sharing information sensibly.
- I will not give out any personal information about myself or anyone else when using the internet.
- If I accidentally come across any material that makes me uncomfortable I will report it to a teacher.
- I will not download or install software.
- I will respect the privacy and ownership of others' work on-line at all times
- I understand the school may watch my use of the school's computer systems and learning platform.
- I understand that I will only be allowed to use the school equipment and systems by following these rules.

Name: ……..……Class……..

Pupil signature:…… Date:……