Buckstones Community Primary School

ICT and internet acceptable use policy

Written and agreed by staff: Monday 5th. September 2022

Adopted by Governors: 20.9.22

Signed by Chair

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), 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 also 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.

Breaches of this policy may be dealt with under our behaviour policy and staff code of conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- 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 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

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

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school’s ICT facilities by any member of the school community.

Unacceptable use of the school’s ICT facilities includes:

- Using the school’s ICT facilities to breach intellectual property rights or copyright
- Using the school’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school’s policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school’s ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school’s filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The head teacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school’s ICT facilities.

4.1 Sanctions

How to respond when a risk is discovered

The head teacher will ensure that the following procedures are adhered to in the event of any misuse of the Internet:

4.1 An inappropriate website is accessed inadvertently:

- Report website to the Headteacher and head teacher.
- Contact the filtering service so that the site can be added to the banned or restricted list.
- Log the incident on cpoms

4.2 An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the Headteacher and head teacher immediately.
- Manager to refer back to the Acceptable Use Policy (Appendix 1) and follow agreed actions for discipline.
- Inform the filtering services as with 4.1 in order to reassess the filters.

4.3 An inappropriate website is accessed deliberately by a child:

- Refer the child to the Acceptable Use Policy that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Log the incident
- Decide on appropriate sanction.
- Notify the parent / carer.
- Contact the filtering service to notify them of the website.

4.4 An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police, social care, CEOP.
- Log the incident.

4.5 An illegal website is accessed or illegal material is found on a computer.

4.5.1 The following incidents must be reported directly to the police:

- Indecent images of pupils found. (Images of pupils whether they are photographs or cartoons of pupils or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
- Incidents of ‘grooming’ behaviour.

- The sending of obscene materials to a child.
- Criminally racist or anti-religious material
- Violent or bomb-making material
- Extremism and radicalisation material (refer to The Prevent Duty)
- Software piracy
- The promotion of illegal drug-taking
- Adult material that potentially breaches the obscene publications act in the UK.
- Harrassment

4.5.2 If any of these are found, the following should occur:

- Alert the Headteacher and head teacher immediately.
- DO NOT LOG OFF the computer but disconnect from the electricity supply.
- Contact the police and or CEOP/ Channel and social care immediately (Police – 0161 856 8962, social care – 0161 770 3790, pupils over 16 – 0161 770 6599, out of hours – 0161 770 6936).
- If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

45.6 An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)

- Ensure the child is reassured and remove them from the situation.
- Report to the manager and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Procedures www.oldham.gov.uk/lscbhome
- Report to the Local Authority Designated Officer (07515188790).
- Preserve the information received by the child if possible.
- Contact the police as necessary.

4.7 Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:

- Preserve any evidence and log the incident.
- Inform the Headteacher immediately and follow Safeguarding Policy.
- Contact the police or CEOP if appropriate.

4.8 Where staff or adults have posted on inappropriate websites, or have inappropriate information about them posted:

- This should be reported to the Headteacher.

4.9 Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

- Preserve any evidence and log the incident on cpoms.
- Inform the Headteacher immediately.

- Check the filter if an Internet based website issue.
- Contact/parents and carers
- Refer to the bullying policy
- Contact the police or CEOP as necessary.

4.10 If images or video of pupils engaged in sexual activity or in revealing poses (sexting) are known to have been posted online the following guidelines should be followed:

- If the images are on a computer follow the guidelines for inappropriate use of ICT equipment. Where the existence of the video or images has come to attention through young people talking about them or viewing them on their phones the following measures should be taken then the Police should be contacted immediately and a CEOP report made giving the available information.
- The incident should be logged through the organisation's own monitoring / line management procedures.
- Appropriate educational/pastoral work should be undertaken with all young people involved.

5. Staff (including governors, volunteers, and contractors)

5.1 Roles and Responsibilities

The governing body

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that school has an effective filtering and monitoring and that alongside the IT provider the effectiveness of the filtering and monitoring systems is checked by school and the IT provider regularly. See Appendix 6.

The headteacher:

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead:

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the ICT Technical Support to put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Working with the Computing leader, technical support and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged using eSafe and/or CPOMs and dealt with appropriately in line with this policy;

- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety and ensuring all staff understand the expectations applicable to their roles and responsibilities in relation to filtering and monitoring;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the governing body.

This list is not intended to be exhaustive.

The ICT Technical Support (Fingertips Solutions)

The ICT Technical Support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use;
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

5.2 Access to school ICT facilities and materials

The school's Business Manager alongside the ICT Technical Support (Fingertips Solutions) manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Business Manager alongside the ICT Technical Support (Fingertips Solutions) manages.

5.2.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be SendSafely encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Head teacher and ICT Technical Support immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

5.3 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The head teacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.6). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 4) and use of email (see section 5.2.1) to protect themselves online and avoid compromising their professional integrity.

5.3.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 4).

5.4 Remote access

We allow staff to access the school's ICT facilities and materials remotely through Google Drive.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school. Staff must ensure their work device is secure and password protected and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of school. Any USB devices must not be used. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy (found in the Policies section of Google Drive).

5.5 School social media accounts

The school has an official Twitter page, managed by head teacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

5.6 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Teaching and Learning

Whilst recognising the considerable benefits of new technologies, we teach pupils to protect themselves from:

- inappropriate content
- undesirable contact
- hurtful conduct

Research indicates that pupils who are given greater freedom at school to use new technologies have a better knowledge and understanding of how to stay safe online. It is therefore important that this school runs a 'managed system' that helps pupils to become safe and responsible users of technology by allowing them to take more responsibility and manage their own risk. We believe that pupils become more vulnerable if they are not given the opportunity to learn how to assess and deal with online risk for themselves.

To support this, the school has adopted the Oldham Charter of Young People's Digital Rights and this is shared widely with pupils in all classes. (See Appendix 2)

6.2 How does on-line technology enhance learning?

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Pupils are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils.

- Access to the Internet may be by teacher or teaching assistant demonstration.

- Pupils may access teacher-prepared materials through the shared folder on the school server or school Intranet, rather than the open Internet.

- Pupils may be given a suitable web page or a single website to access.

- Pupils may be provided with lists of relevant and suitable websites.

- Older, more experienced pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher. Pupils will be expected to observe the rules for acceptable use.

Pupils accessing the Internet will be supervised by an adult at all times.

6.3 Pupils will be taught to evaluate Internet content

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that most of the information on the Internet is intended for an adult audience and that much of the information on the Internet is not properly audited/edited. Pupils will 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 to expect a wider range of content, both in level and in audience, than is found in the school library or on TV.

- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium).

- When copying materials from the Internet, pupils will be taught to observe copyright.

- Pupils will be made aware that the writer of an e-mail or the author of a webpage may not be the person claimed.

6.4 Online safety education / 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 online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience. They also need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.

- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.

- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school. (See appendix 4)

- Staff and volunteers should act as good role models in their use of digital and online technologies and are required to sign an Acceptable Use Agreement. (See appendix 3)

- 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, staff should be vigilant in monitoring the content of the websites the young people visit.

6.5 Access to ICT facilities

- "Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff"
- "Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff"
- "Pupils will be provided with an account linked to the school's virtual learning environment e.g. Google classrooms, Abacus maths., SPaG.com etc.

6.6 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.7 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 Roles and Responsibilities

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet;

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

• What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

7.2 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the Friends of Buckstones) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.3 Communicating with or about the school online

- Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours yet many have a limited understanding of online safety risks and issues. Parents may under estimate how often their children come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:
- • Curriculum activities
- • Letters, newsletters, website,

- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the head teacher immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data daily and store these backups on cloud based backup systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Fingertips Solutions
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on

10. Internet access

The school wireless internet connection is secured.

Whilst providing children with a safe environment in which to learn, we will be doing all that we reasonably can to limit children's exposure to risks from the school's IT system. As part of this process, we implement monitoring systems through a monitored Firewall to detect any inappropriate use of the internet. See Appendix 6.

All staff have a responsibility to log behaviour and safeguarding issues related to online safety on CPOMs which will be monitored by the DSL.

10.1 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the Friends of Buckstones)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Parents and visitors will not be permitted to hotspot as this bypasses the school's wifi and the filtering that is in place.

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 3 years.

12. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning
- Mobile phone usage

To be reviewed every 3 years.

Appendix 1

Acceptable Use Policy

Early Years and Key Stage 1

I understand that Buckstones Acceptable Use Policy will help keep me safe and happy online whether I am using school devices or my own personal devices.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know that Buckstones staff can see what I am doing online when I use computers and tablets and Tapestry, Google Classrooms, Purple Mash, etc. including when I am at home.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules my teacher will:
    - restrict or remove access to the internet, my remote learning platform and devices,
    - inform my parents/carers, only give me access to hard copies of my school work.
- I have read and talked about these rules with my parents/carers.

Key Stage 2

I understand that Buckstones Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I will always be myself and not pretend to be anyone or anything I am not.

Learning

- I will use tablets, laptops to access online learning.
- I will not use a personal device to access the internet and only use school equipment.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work.

- If I need to learn online at home, I will follow the school remote learning AUP.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will log off when I have finished using the computer or device.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.
- I will not look for bad language, inappropriate images or violent or unsuitable games and, if I accidently come across any of these, I will report it to a teacher or adult in school, or a parent or carer at home.
- If, for any reason, I need to bring my mobile phone into school, I know that it is to be handed in to the office and then collected at the end of the school day.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then:
  - restrict or remove access to the internet, my remote learning platform and devices,
  - inform my parents/carers,
  - contact the police if a criminal offence has been committed.
  - only give me access to hard copies of my school work.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

I understand that:

- these expectations are in place to help keep me safe when I am learning at home using Google Classrooms, Zoom, Purple Mash, TT Rock Stars, SPaG.com, Tapestry etc.
- I should read and talk about these rules with my parents/carers.
- remote learning will only take place using Google Classrooms, Zoom, Purple Mash, TT Rock Stars, SPaG.com and during usual school times.
- My use of Google Classrooms, Zoom, Purple Mash, TT Rock Stars, SPaG.com is monitored to help keep me safe.

2. Only members of Buckstones community can access Google Classrooms, Zoom, Purple Mash, TT Rock Stars.

- I will only use my Buckstones provided login details to access remote learning.
- I will use privacy settings as set up the school.
- I will not share my login/password with others.
- I will not share any access links to remote learning sessions with others.
- When taking part in remote learning I will behave as I would in the classroom. This includes:
  - Using appropriate language.
  - Not taking or recording any images or content.
  - Not sharing images or other work as my own.
  - Having an appropriate avatar.

4. When taking part in Zoom sessions I will:

- Mute my microphone when asked to.
- Wear appropriate clothing and be in a suitable place.
- Ensure backgrounds are neutral and personal information is not visible.
- Use appropriate alternative backgrounds.
- Attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
- Attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.
- Have my own name as a screen name.

5. If I am concerned about anything that takes place during remote learning, I will:

- Report my concerns to my teacher and tell a parent/carer.

6. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:

- Restricting or removing access to my remote learning platform and devices,
- Informing my parents/carers,
- My teacher contacting police if a criminal offence has been committed.
- Only having access to hard copies of my school work.

Appendix 2

Buckstones Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the Buckstones Acceptable Use of Technology Policy (AUP) and remote learning AUP.

I agree to follow the AUP when:

1. I use Buckstones devices and systems, both on site and at home.

2. I will not use my own devices in Buckstones, including mobile phones, gaming devices and cameras.

3. I may use my own equipment outside of Buckstones, including communicating with other members of the school or when accessing school remote learning systems.

Name…….

Signed……..

Class……

Date…….

Parent/Carers Name……

Parent/Carers Signature……

Date……

Appendix 3

Contract for Acceptable Use of the Internet (Staff/Volunteer)

- I know that I should only use school equipment in an appropriate manner.
- I know that images should not be inappropriate or reveal any personal information of pupils and young people if uploading to the Internet.
- I have read the school e-safety and acceptable use policy so that I can deal effectively with any problems that may arise.
- I will report accidental misuse to the Headteacher.
- I will report any incidents of concern for the pupil's safety to the Headteacher, designated person for child protection in accordance with the e-safety and acceptable use policy.
- I know the designated person for child protection is Sarah Healey and in her absence Melanie Platt.
- I will ensure that personal data (such as data held on SIMS) is kept secure and I follow the Data Protection Act 1998.
- I know that I am putting myself at risk of misinterpretation and allegation if I contact pupils and young people via personal technologies, including my personal e-mail and phone and should use the school e-mail and phones (if provided) and only to a child's school e-mail address if possible.
- I will ensure that I keep my password secure and do not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

Name: ……

Signed: ……

Position: ……Date: ……

Appendix 4

Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional

3. Check your privacy settings regularly

4. Be careful about tagging other staff members in images or posts

5. Don't share anything publicly that you wouldn't be just as happy showing your pupils

6. Don't use social media sites during school hours

7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there

8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)

9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this

Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to Facebook or the relevant social network and ask them to remove it

If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 5

Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.

Appendix 6

Buckstones Primary School
Internet Filtering and Monitoring Provision, 2023.

All internet access within the school, is subject to checking by our Watchguard M270 Firewall. This device runs specialist filtering software, called WebBlocker. WebBlocker is a "category based filter", which means that we select categories of content that are considered undesirable and any website which matches this category gets blocked.

If a website is blocked, this access is logged on an external service called Dimension. These attempts to access a website in a blocked category are visible to the school's designated safeguarding lead (DSL), as well as the team at Fingertip Solutions. We can see the site that was blocked, the time of the attempted access and which device was being used at the time.

The system also enforces "safe search" on both Google and Bing search engines.

The senior leadership team determine the categories of blocked content, and this is reviewed on a regular basis. The decisions are made on the basis of wishing to prevent access to the most inappropriate content whilst ensuring that valuable teaching resources are not impacted. If you find that an appropriate site is being incorrectly blocked, please bring it to the attention of your designated safeguarding lead and we can organise to whitelist the site in question. Likewise, if you find a website that contains inappropriate content that hasn't been blocked by the filter, let us know and we can blacklist the site.

At the time of the most recent review, the following categories of content are blocked by the filter within your school: Abortion (Pro-Choice and Pro-Life), Adult Content, Adult Material, Lingerie & Swimsuit, Nudity, Sex, Sex Education, Abused Drugs, Drugs, Marijuana, Nutrition (Drugs), Prescribed Medications, Dynamic DNS, Elevated Exposure, Emerging Exploits, Extended Protection, Newly Registered Websites, Suspicious Content, Gambling, Proxy Avoidance, Intolerance, Militancy and Extremist, Parked Domain, Advanced Malware Command & Control, Bot Networks, Compromised Websites, Keyloggers, Malicious Embedded Link, Malicious Embedded iFrame, Malicious Websites, Mobile Malware, Phishing and Other Frauds, Potentially Unwanted Software, Security, Spyware, Suspicious Embedded Link, Alcohol and Tobacco, Personals and Dating, Sport Hunting and Gun Clubs, Tasteless, Violence, Weapons.