

Issue date: March 2019 Reviewed May 2020 / Sept 2022 / April 2024 / Sept 2025
Date adopted: 25 th March 2019
Signed by: Full Governing Board
Approval committee: Governing Body



Burton CE Primary

School

Computing, Acceptable Use and Safer Digital Practices policy

Computer Co-Ordinator – Amber Jones / Julia Kolbucaj

1. Introduction

At Burton CE Primary School we value the contribution that Computing can make for the benefit of all pupils, staff, parents and governors. We strive to provide opportunities for computing in all subjects to motivate and inspire pupils and raise standards across the curriculum. Everyone in our school community will become lifelong creators and learners, equipped to meet developing technology with confidence, enthusiasm and the skills that will prepare them for a future in an ever-changing world.

UNICEF Article 17, “Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand and should not promote materials that could harm children.”

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. The use of these technologies can put young people at risk within and outside school. All members of the Burton Primary School community should have an entitlement to safe internet access at all times.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always act primarily to safeguard pupils in school and will advise the head teacher of the justification for any such action already taken or proposed. The head teacher/SLT will in turn seek advice from the schools’ HR or local Safer Schools team where appropriate.

This Policy operates alongside our Safeguarding/ Child Protection Policy; Whistleblowing Policy; Mobile Technology Policy; Staff Code of Conduct; Procedures for dealing with Youth Produced Sexual Imagery and other relevant policies to ensure the safety of our pupils.

2. Aims and objectives

We aim to enable our staff and pupils to become competent, confident and independent users of information and communication technologies; To provide pupils with the skills necessary to become independent learners; To develop a creative and cross-curricular approach to the teaching and learning of information and communication technologies; To promote safe and responsible use of information and communication technologies through a programme of digital literacy; To use new technologies to enable good quality teaching and learning to take place; To ensure safe, appropriate and equal access of information and communication technologies for all children regardless of age, gender, ethnicity or ability; To ensure our pupils take advantage of the ever quickening pace of technological change by ensuring our children are inspired to evaluate their work, and to analyse and develop their own methods of using information and communication technologies to solve problems or complete a task in the best

way. To provide pupils with an understanding of the role information and communication technologies have in everyday life at present and their importance in the future.

Curriculum:

3. The school's curriculum organisation

We use a topic based curriculum approach to teach units of work; computing is an ideal means by which to support and enrich learning in this way. Computing is integrated into topics where possible, but some aspects are taught as standalone units of work (See Long Term Curriculum Plan). It is the responsibility of the teachers to ensure that their units are taught appropriately, and that planning includes Computing Learning objectives. It is the responsibility of the computing coordinator to ensure coverage of the objectives across the year groups and that appropriate resources and training are provided.

4. Curriculum Management

The Subject Leader will facilitate the use of computing by:

- Updating the policy and the units of work.
- Monitoring the curriculum
- Supporting staff in developing pupils' capabilities
- Keeping staff abreast of new developments
- Attending appropriate courses to update knowledge of current knowledge and attending Pyramid curriculum meetings.
- Ordering and updating resources
- Supporting other subject leaders in developing Computing within their subject
- Liaising with the School Business Manager and the technician to support the computing equipment.

5. Access to Computing

All members of Burton Primary School's community are expected to be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use. Our school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school has a Wi-Fi enabled network in all teaching areas. Each class room has an interactive display panel. Teachers can access the school's network off site via the 'cloud' based remote log in using their encrypted laptops.

All teachers have password protected class iPads to support their role with a selection of apps. There are a number of pupil iPads, all of which can be used flexibly to support learning inside or outside (equipment can be booked in advance to ensure it is available).

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter (as indicated in our Code of Conduct).

Pupils' use of our equipment should always be in accordance with our policy, where use should be guided and supervised. There are a variety of other pieces of equipment such as programmable floor robots which are available. Laptops are linked to central printers in the staff room and library. Printing is accessed via an individual code which ensures sensitive information is kept secure

6. Inclusion

The computing curriculum is available to all children, whatever their ability. It forms part of the school teaching and learning policy to provide a broad and balanced education to all children. Through our teaching we provide learning opportunities that match the needs of children with learning difficulties

and we take into account the targets set for individual children. Our ICT facilities are a great support when facilitating the learning of all children.

7. Health and Safety

Staff and children are shown how to use equipment appropriately. Guidance for ensuring the safety and security of all users is reinforced through the teaching of e-safety.

8. Copyright and Licensing

All users of ICT equipment are required to abide by the legal requirements and limits laid down in copyright legislation. Where necessary, eg use of music for worship & school productions, a license will be purchased.

9. Reporting Learning

Children's progress is assessed by teachers in the course of their teaching, through observation, questioning and analysis of work. It is the responsibility of the class teacher to assess the progress of individual learners. This involves identifying each child's progress, determining what each child has learned and what, therefore, should be the next stage in his/her learning, so informing future planning. Parents are informed in our summer term reports of their child's progress.

10. Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's computing provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. All members of Burton Primary School's community are aware of the dangers they may face from the four main areas of risk (as outlined in Keeping Children Safe in Education) in their use of digital technology. Within the areas of content, contact, conduct and commerce, these may include:

- a) Access to illegal, harmful or inappropriate images or other content – including radicalisation.
- b) Unauthorised access to; loss of; or sharing of personal information
- c) The risk of being subject to grooming by those with whom they make contact on the internet.
- d) The sharing or distribution of personal images without an individual's consent or knowledge
- e) Inappropriate communication or contact with others, including strangers
- f) Cyber-bullying / online bullying
- g) Access to unsuitable video or internet games
- h) An inability to evaluate the quality, accuracy and relevance of information on the internet.
- i) Plagiarism and copyright infringement
- j) The risks of online gambling; phishing and financial scams
- k) The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Online Safety Pupils:

All children are taught how to keep themselves safe when using digital technology. The digital leaders help to ensure this message is high priority and understood by all pupils. The computing leader has CEOP training and as a NOS (National Online Safety) School all staff have access to training and resources to support the teaching of E-safety

Online Safety education will be provided in the following ways:

- A planned e-safety curriculum is provided in every year group as part of the Computing curriculum through National Online Safety Key Stage packs; along with workshops provided by the Safe Schools and Community Team (SSCT).
- E-Safety is also part of PHSE and other lessons and is regularly revisited

- Each year, Safer Internet Day is observed as an important part of our way of supporting the children in being safe online.

Online Safety – Parents and Carers:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- Ensuring the Online Safety for Parents & Carers Course from National Online Safety is made available to our School Community
- Parent E-Safety Workshops delivered by SSCT or similar external provider
- Letters
- newsletters
- School website
- Reference to the SWGfL Safe website
- Highlighting National Online Safety leaflets that are relevant to families through the Newsletter and website
- Video links on the website to support families with Safer Internet Day
- Individual phone calls where circumstances warrant this

Online Safety – Staff:

- Staff are expected to complete e-safety training annually delivered by National Online Safety, for which they will receive a certificate and the computing lead will be notified of completion.
- Staff are expected to understand their responsibilities, as outlined in this policy.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand Burton Primary School's Computing, Acceptable Use and Safer Digital Practices Policy.
- This policy and its updates will be presented to and discussed by staff in staff meetings.
- The Computing Co-ordinator (or other nominated person) will provide advice / guidance / training as required to individuals.
- All staff to sign and date the Acceptable Use Agreement Document.

Staff will monitor the use of digital technologies, mobile devices, cameras etc in lessons. Where internet use is pre-planned - in class or for remote learning / home learning - pupils should be guided to sites checked as suitable for their use and staff should ensure that processes are in place for dealing with any unsuitable material that is found.

Where children are interacting with others online as part of their learning (remote learning; use of webinars etc) this will usually be with known adults e.g members of staff and every effort should be made to ensure that other children, another adult or parents are also present.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build, pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Community Users who access school systems / website as part of the wider school provision will be expected to sign the Acceptable Use agreement before being provided with access to school systems.

11. Cyber-bullying:

Cyberbullying – staff:

- Cyberbullying is defined by Unicef as “bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:
 - spreading lies about or posting embarrassing photos or videos of someone on social media
 - sending hurtful, abusive or threatening messages, images or videos via messaging platforms
 - impersonating someone and sending mean messages to others on their behalf or through fake accounts.”
- Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.
- If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site. Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process.
- Staff are expected to report all incidents of cyberbullying to their line manager or the head teacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Cyberbullying – Pupils:

- Designated Safeguarding Lead (DSL) for child protection and Deputy DSL should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from cyberbullying.
- All members of staff have responsibility to respond to reports of cyberbullying by another pupil by informing parents and through seeking advice from the head teacher, DSL and the Safer Schools and Community Team.
- Pupils should be helped and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils need to understand the importance of reporting abuse, misuse and any cyberbullying issues which arise from their digital practices.

12. Social Networking:

- Social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, Instagram and Snapchat are perhaps the most well-known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.
- All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues,

pupils or students, public in general and all those with whom they work in line with the school's code of conduct.

- Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.
- Managing personal information effectively makes it far less likely that information will be misused.
- In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.
- All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.
- Staff are advised to regularly check their security settings.
- Staff should never 'friend' a pupil at the school where they are working onto their social networking site.
- Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.
- Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.
- Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about the school, other employees, pupils or other individuals connected with the school, or another school, or local government could result in formal action being taken against them.
- Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications; and that email communications can be requested as part of a personal data Subject Access Request under GDPR regulations.
- Staff must never post derogatory remarks or offensive comments on-line or engage in online activities which may bring the school or local government into disrepute.
- Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.
- Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.
- There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school/setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
 - Read and understand our Acceptable Use Policy.
 - Where they are running official accounts, sign our social media Acceptable Use Policy.
 - Be aware they are an ambassador for the school/setting.
 - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
 - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
 - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - Not engage with any private or direct messaging with current or past learners or their family members.
 - Inform their line manager, the DSL (or deputy) or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners
- We will empower our learners to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- Learners will be advised:
 - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
 - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
 - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
 - to use safe passwords.
 - to use social media sites which are appropriate for their age and abilities.
 - how to block and report unwanted communications.
 - how to report concerns on social media, both within the setting and externally.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.

13. Use of Digital and Video Images

- There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.
- Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.
- Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools and schools' staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential.

- Where indecent images of children are found by staff, the police and local authority designated officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.
- Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the LADO should be informed and advice sought. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate or evaluate the material themselves until such advice is received.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow this policy and refer to parental permissions concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used to store images of children.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission and only in relation to school approved activities and on school equipment.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Children's images may be used on the website unless parents have indicated otherwise.

14. Communication between Pupils/School Staff:

- Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.
- This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.
- It is the expectation that the school should provide a work telephone and e-mail address for communication between staff and parents. Staff should not give their personal mobile numbers or personal e-mail addresses to pupils or parents.
- Staff should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.
- Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.
- Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.
- E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with this policy.
- School may hold personal mobile numbers for pupils in Year 5 and 6 who have permission to walk to or from school. These will be held in the office and only used to contact children where there are concerns – eg about the child's whereabouts if they have failed to arrive at school - and contact cannot be made via the normal communication routes with parents/ carers.

15. Data Protection (To be read in conjunction with the Data Protection Policy):

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and updated 2018 GDPR regulations; which state 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.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

16. Roles and Responsibilities:

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors:

- Governors are responsible for reviewing the effectiveness of this policy. The Safeguarding Governor is responsible for the audit of all policies relating to E-Safety and this is included in the annual cycle of events for safeguarding. The Governor responsible for safeguarding will receive regular information about online safety incidents and monitor reports. At least 1 governor will have completed the NOS online training.

Headteacher and Senior Leaders are responsible for:

- Ensuring the safety (including e-safety) of members of the school community, although the day to day responsibility for e-safety will be delegated to the Computing Co-ordinator.
- Ensuring that the Computing Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Ensuring that they are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (Refer to Burton Primary School policy, Allegations Made Against Staff)
- Ensuring key e-safety messages are reinforced as part of a planned programme of assemblies.
- Ensuring pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Teaching and Support Staff are responsible for:

- Ensuring they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices including school procedures for dealing with Youth Produced Sexual Imagery (see policy).
- Ensuring they report any suspected misuse or problem to the Computing Co-ordinator or Headteacher for investigation / action / sanction.
- Ensuring that any digital communications with pupils (email /website / voice) should be on a professional level and only carried out using official school systems.
- Ensuring that e-safety issues are embedded in all aspects of the curriculum and other school activities. Ensuring that pupils understand and follow the school's acceptable use policy.
- Ensuring that all pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Ensuring that they monitor ICT activity in lessons, extracurricular and extended school activities.
- Ensuring that they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- Ensuring pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Pupils are expected to:

- Be responsible for using the school ICT systems in accordance with the Acceptable Use ICT Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations understand the need and importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Know and understand the school policy on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking or use of images.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy is applicable to keeping them safe wherever they are and that the Acceptable Use Policy covers their actions out of school, if related to their membership of the school.

Computing Co-ordinator is responsible for:

- Taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff and Digital Leaders
- Liaising with school ICT technical staff (Turn IT on)
- Receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- Meeting regularly with the Digital Leaders to support their training and also with the Safeguarding Governor to discuss current issues and review incident logs.

Network Management:

The Headteacher and Computing Co-ordinator are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant local authority guidance.

- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- Smoothwall and Trailblaze is informed of issues relating to the filtering applied by Smoothwall.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network / remote access / email is regularly monitored in order that any misuse can be identified and prevented.
- Pupils should be helped and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Staff should be vigilant in monitoring the content of websites that pupils visit.

Policy Review:

This Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Should serious E-Safety incidents take place, the following external persons or agencies will be informed: BCP LA, BCP Safeguarding Officer, Police Commissioner's Office, Smoothwall, Trailblaze, Safer Schools Team.

Acceptable Use Policy Agreement –Staff Members

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I have read and understood the Computing, Acceptable Use and Safer Digital Practices policy

I understand that:

- Burton Primary School will monitor my use of the systems, devices and digital communications.
- I must keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I must immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Everyone has equal rights to use technology as a resource and that Burton Primary School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I should not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I must not use Burton Primary School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a senior member of staff to do so.
- I should act as I expect others to act toward me:
- I should respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I must be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I must not take or distribute images of anyone without their permission or in the case of children, their parent's permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Burton Primary School:

Use of mobile phones (or other personal digital equipment).

- It is the policy of Burton Primary School, that mobile phones (or other digital equipment) should not be brought to school by pupils unless the child is walking to and from school independently. Before accessing the school they must hand their phone into the school office for the duration of the day.
- I understand that, if I do use my own devices in Burton Primary School, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- Personal devices must be password/code or fingerprint protected
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings unless I have permission to do so.

- I will only use social media sites with permission and at the times that are allowed (during break times and only when not supervising pupils).
- Phones may only be used during lesson times for legitimate reasons such as using timer functions or to access support via the TEAM SOS app.
- I will not have my phone available for personal calls during time I am with the children except by prior permission of the Headteacher or a member of the Senior Leadership Team.

Network security

Users are expected to inform their class teacher or ICT Co-ordinator immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password and must not share this information with other users. Users identified as a security risk will be denied access to the network.

Physical security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when taken off the school premises. When transporting laptops in cars, they are to be locked in the boot for secure storage. Laptops and iPads taken out of school should be encrypted or password protected.

Wilful damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

Media publications

Named images of pupils (e.g. photographs, videos, web broadcasting, TV presentations, web pages etc.) must not be published under any circumstances.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and must comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Children's images (including videos, TV presentations, web pages, etc.) may be used on the website unless parents have indicated otherwise on the Consent for Use of Images form.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

- I have read the policy and I understand that I am responsible for my actions, both in and out of school:
- I understand that Burton Primary School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this 'Computing, Acceptable Use and Safer Digital Practises Policy', I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

.Signed _____

PRINTED NAME _____

CLASS: Pupil Acceptable Use Policy Agreement Template

I understand that for my own safety:

- Adults at school will monitor my use of the digital equipment and any messages I send.
- I must keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password

When we use computers/iPads:

- I will ask a teacher or member of staff if I want to use the computers/iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer/iPad and other equipment
- I will always treat others online in a kind and appropriate way.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or member of staff if I see something that upsets me or I think is inappropriate on the screen.
- I know that if I break the rules I might not be allowed to use a computer in school.

When I use computers at home and at school:

- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will not arrange to meet people off-line that I have communicated with on-line; If I am asked to, I will speak to an adult.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

- If I am allowed to bring a phone to school (Year 5 & 6 only), I will not use it on school property without my teacher's express permission and will hand it in to be kept safe during the school day.

This policy agreement has been shared during a class council meeting.

Sign_____

PRINTED NAME_____

(Class/ Pupil Governor Representative)