E-Safety policy

Date presented to Governors: **Spring Term 2018**

Review date: **Spring term 2021**

Signed Ms *S Ward* **Signed** *Mrs F Good*

Headteacher **Chair of Governors**

E-safety policy

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

This policy should be read in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

E-safety co-ordinator: Miss A Wright

At Burton Pidsea Primary School we will take all reasonable precautions to ensure E-safety. However, owing to the international scale and nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning. This policy explains how we try to keep pupils safe in school and protect and educate them in the safe and appropriate use of technology. Behaviours such as cyber bullying and sexting will be managed through the Anti-bullying or Child protection policy and procedures.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working
- will use existing, as well as up and coming, technologies safely.

E-safety

Pupils will be taught about e-safety, and will be taught how to report any inappropriate web content. E-safety rules will be produced by children where applicable and will be posted in each room where a computer is used.

The school will communicate and publicise e-safety issues to parents through the school newsletter, website and consultation evenings. The E-safety co-ordinator will establish and maintain a staff professional development programme relating to E-safety as well as a parental awareness programme.

All staff are aware of and know when and how to escalate incidents concerning E-safety issues (see below); any instances of pupil internet misuse should be reported to the head teacher. The head teacher will also consult with the ERYC IT support team to ensure such misuse cannot happen again. The Governing Body may also be informed of any e-safety issues and policy developments.

Use of the internet in the classroom

Filtering systems are managed by the ERYC IT service but we are fully aware that these filters are not infallible and staff are aware that effective monitoring is essential (including the keeping of a log of inappropriate content). We understand that this situation has a level of risk, but an 'over blocking' system would prevent the effective teaching of online safety and resilience. The analogy would be that children will never learn to swim safely without taking them to the swimming pool.

Staff will utilise the internet to support, extend and enhance learning and pupils will be given have opportunities to engage in independent and collaborative learning using the internet and other digital technologies, including how to effectively use the internet for research purposes. Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

When planning for internet use, staff will ensure:

- pupils are given clear objectives for internet use
- web content will be age-appropriate
- good practice in using new and emerging technologies is modelled
- E-safety is highlighted regularly in the curriculum.

E-mail

Pupils will only use a school e-mail for approved activities.
Pupils and staff will only use approved e-mail accounts when using the school network. Pupils will tell a member of staff if they receive inappropriate e-mail communications and staff will follow the school procedure for reporting E-safety concerns.

Acceptable use

Staff will read and sign the ICT Acceptable Use Policy, laptop protocol and Mobile Phone policy before using any school ICT resource.
Parents and children will read and sign an internet access consent form and Acceptable Use Policy before their children are given access to internet resources.

(see also Anti-bullying policy)

Mobile phones

All staff have read and signed the school Mobile Phone policy
Children are not permitted to keep mobile phones and other handheld technology within school. If children are required to carry a mobile phone on their journey to and from school, then the phones should be switched off and handed into the office at 8.50am and collected at 3.30pm

Role of the E-safety co-ordinator

At Burton Pidsea Primary School, we aim to establish and maintain a safe ICT learning environment. The Head Teacher will ensure that appropriate time and funding is allocated to support e-safety activities throughout the school and, working together with the e-Safety co-ordinator will establish and maintain a school-wide e-safety programme and develop and review e-safety policies and procedures. The E-safety co-ordinator will respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.

Reporting E-safety concerns

If staff are aware of the misuse of IT equipment and/or the internet, they should inform the E-safety co-ordinator or Head Teacher. Allegations will be investigated using the E-safety concerns guidelines (Appendix 5).

The possible consequences for such actions include:

- informing parents or carers
- removal of Internet or computer access for a fixed period
- referral to Local Authority
- We will contact the Police if one of our staff or pupils sends or receives online communication that we consider is particularly disturbing or breaks the law

Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with our Child Protection procedures.

The wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's processes documented above.

The final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

Please read this policy in conjunction with:
Anti bullying policy
Safeguarding policy
Teaching and learning policy
Subject specific policies

Burton Pidsea Primary School

Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep **SECRETS**-just because someone asks me to	
7. I don't change my **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

At school, my trusted adults are:

_____

At home, my trusted adults are:

_____

My name is _____

Date received at school office: _____

Burton Pidsea Primary School

Key Stage 2: Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.

- ***I am a secure online learner*** – I keep my passwords to myself and will have them reset them if anyone finds them out.

- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.

- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.

- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.

- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.

- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.

- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.

- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.

- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different from me. If I see anyone doing this, I tell a trusted adult.

- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.

- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.

- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.

- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.

- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.

- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Signed: _____ Date: _____

Parents / carers

I am aware I can visit:

- www.thinkuknow.co.uk/parents
- www.nspcc.org.uk/onlinesafety
- www.internetmatters.org
- www.saferinternet.org.uk
- www.childnet.com

for more information about keeping my child(ren) safe online

Parents / carers signature: _____

How will E-safety infringements be handled?

Whenever a student or staff member infringes the E-safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

STUDENT	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised mobile phone/personal device in classroom	Refer to class teacher
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised mobile phone/personal device in classroom • Accidentally accessing offensive material and not notifying a member of staff of it	Refer to E-safety co-ordinator / Head teacher Escalate to: • informing parents or carers • removal of Internet or computer access for a fixed period
Category C infringements	**Possible Sanctions:**
• Sending an email or message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or inappropriate material (one-off)	Refer to Head teacher Escalate to: • informing parents or carers • removal of Internet or computer access for a fixed period • referral to Local Authority • contact the Police if offence is considered particularly disturbing or breaks the law **Other safeguarding actions** If inappropriate web material is accessed, ensure appropriate technical support filters the site Inform LA IT services

Category D infringements	Possible Sanctions:
• Continued sending of emails or messages regarded as harassment or of a bullying nature • Deliberately creating accessing, downloading or disseminating any material deemed offensive, inappropriate, defamatory, racist, homophobic or violent • Sharing or requesting of images that would be considered inappropriate. • Bringing the school name into disrepute	Refer to Head teacher Escalate to: • informing parents or carers • removal of Internet or computer access for a fixed period • referral to Local Authority • contact the Police if offence is considered particularly disturbing or breaks the law **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform LA IT services • Inform the service provider if appropriate. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, social networking etc. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Lack of due care resulting in infection or distribution of viruses or malware • Misuse of first level data security, e.g. sharing of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	Referred to Head Teacher & HR Escalate to: • Verbal or written warning given
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school computer hardware or software • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	Referred to Head Teacher & HR Referred to Governing Body Escalate to: • Report to LA IT services • Report to Police / CEOP where child abuse or illegal activity is suspected. • HR advice regarding disciplinary procedures **Other safeguarding actions:** • Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. • Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. • Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct

A full and thorough investigation will be actioned before disciplinary action is taken for any alleged offence.
As part of the investigation, the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

However, the head teacher reserves the right (after consultation with HR) to instantly suspend the member of staff concerned if the safety of the children or staff is deemed to be at risk.

The school will involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff will be **immediately suspended** and the Police will be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

Burton Pidsea Primary School
Staff Acceptable Internet Use Policy

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided.
All staff should follow the guidelines at all times.
You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes as agreed by the School senior management team.

- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them.

- Any online activity should not harass, harm, offend or insult other users.

- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.

- You should not download or install any hardware without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.

- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher

- Any electronic communications with pupils or parents should be related to schoolwork only, and should be through school e-mail addresses or other school systems e.g. learning platforms. It is not acceptable to contact pupils (or ex-pupils who are under 18) using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.

- Any online activity, including messages sent and posts made on websites (including social media), and including activity outside of school, should not bring your professional role or the name of the school into disrepute.

- Any still or video images of pupils and staff should be for professional purposes only. They should be stored, transferred to and used on school equipment. Such images should not be stored on personally owned computers.

- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.

- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.

- Personal or sensitive information should only be taken off-site if agreed with the head teacher, and steps should be taken to ensure such data is secure. Your laptop must have a password protected username login.

- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.

- You should support and promote the school e-safety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching.

Finally:

- You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.

✂----------

I confirm that I have read and understood the Burton Pidsea Primary School
Staff Acceptable Internet Use Policy for Teachers & Support Staff

Name (Printed): ……. Signed : ……

Date: ……

Please return this tear off slip to the school office

Burton Pidsea Primary School
Laptop Protocol for Teachers and School Support Staff

This protocol is designed to act as a guide and simple framework upon which the use of laptops by teachers or school support staff should be based. The intended spirit of the list is to act as a reminder on use and security.

- The ownership of the laptops rests with the school.

- Teachers / support staff have full use of the laptops to develop planning, curriculum subject and ICT experience.

- Teachers / support staff are reminded that they should not deliberately seek out inappropriate / offensive materials on the internet and that they are subject to the LA's disciplinary procedures for teaching and non-teaching staff should they do so.

- Anti-virus software is provided with each laptop and members of staff have the responsibility of keeping the software up-to-date and for scanning materials downloaded from the internet.

- Teachers / support staff should save work on encrypted usb memory sticks rather than on the laptop itself. This should then be backed up to the school server. No personal data should be saved onto the laptop. This way there will be no risk of a data breach if the laptop is lost, damaged or stolen.

- There are a number of legal requirements relating to the use of information and software (e.g. Data Protection Act, Copyright Act). Teachers / support staff are responsible for understanding and complying with their legal requirements. Training in data protection will be given.

- Teachers / support staff should be aware that laptop computers have a high re-sale value and that they should never be left in cars or in a place where an opportunist could take it. With most insurance companies laptops are covered in cars as long as they are not left unattended.

- Teachers / support staff should make sure that they are aware of the arrangements that have been made by the school for insurance cover on laptop computers and to follow any guidelines / procedures established by the school to safeguard this cover.

- Be aware of the school's policy on the use of laptops and the school network.

✂----------

I confirm that I have read and understood the Burton Pidsea Primary School
Laptop Protocol for Teachers & Support Staff.

I agree to abide by the guidelines and procedures outlined.

Name (Printed): ……. Signed : ……

Date: ……

Please return this tear off slip to the school office

Burton Pidsea Primary School
Staff Mobile Telephone policy

- Personal phones and electronic equipment are to be stored out of pupils sight e.g. classroom cupboard. They must be turned to 'silent'.
- Personal phones are not to be used in front of the pupils.
- Children should not be allowed to view or hear anything from your personal phone
- Personal phones should not be used to take images of pupils.
- Personal calls and messages should only be taken during break periods, unless they are an emergency. If on the school premises, these should take place in the staff room, an empty classroom or in the PPA room
- On school visits staff should take a phone to stay in contact with school. The number should be left with the office.

✂----------

I confirm that I have read and understood the Burton Pidsea Primary School
Mobile telephone policy for Teachers & Support Staff

I agree to abide by the guidelines and procedures outlined.

Name (Printed): ……. Signed : ……

Date: ……

Please return this tear off slip to the school office