Burford CE Primary School

E-safety Policy

October 2025

Headteacher's signature: E Partridge

Chair of Governing Body signature: A Teale

This policy has been created in line with our core Christian values:

At Burford we are

Rooted in love,

Becoming me, and

Flourishing together.

This e-safety Policy is written with our Christian Values of Love, Trust and Courage in mind at all times.

We trust the children, parents and staff within our community will show courage by not accepting poor behaviour online from themselves or others. They will show love to themselves and others through positive behaviour role modelling. Through living their Christian values the children will be responsible and careful computer users respecting the school and wider community.

Responsibilities

The member of SLT team responsible for e-safety is Emma Partridge

The e-safety subject lead is Molly Wildman

The e-safety subject leader is responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the community. He/she may also be required to deliver workshops for parents. The e-safety subject leader is responsible for feeding back to: SLT, governors, teaching staff, admin staff, parents and pupils.

Internet use and Acceptable Use Policies (AUPs)

All members of the school community will sign an Acceptable Use Policy that is appropriate to their age and role. Examples of the AUPS used can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip. This can be found in appendix 2

AUPs will be reviewed annually. All AUPs will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images.

Staff should always use a school camera/Ipad to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection Act.

Mobile Phones and Camera Use within the whole school including Early Years

To ensure the safety and welfare of children in our care, personal mobile phones are not permitted within our setting when in the presence of children.

All mobile phones must be kept in a secure place and should not be accessed throughout contact time with the children.

Photographs or images of any children within our care may only be taken following parental consent and only using the school camera/Ipad and those images should remain within this setting.

When on outings, mobile phones may only be used to make or receive phone calls relating directly to ensuring the safety and wellbeing of the children.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background unless they have asked permission from their guardians.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2).

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Use of e-mails

Pupils and staff should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils and staff are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'). Pupils from Y3-Y6 are provided with their own login to access their secure system and must not share their logins with other children.

All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to used in school. Staff need to risk assess any data that they plan to temporarily store on a USB pen to ensure that any potential loss has minimal impact. Further details regarding this can be found in the Information and Governance Policy. (see appendices) Staff are able to access 'Staff Share' from home but must be careful when downloading confidential data.

Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting sheet that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying) should be reported to SLT in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg CEOP button, trusted adult, Childline).

Infringements and sanctions

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.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to 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.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. class commendation for good research skills, certificates for being good cyber citizens etc.

Social networking

Pupils

Pupils are not permitted to use social networking sites within school.

Staff

It is recognised that social networking sites have a major role to play in today's society.
However, staff must be aware of the following:

Staff must not add pupils as friends in social networking sites.
Staff must not post pictures of school events without the Headteacher's consent
Staff must not use social networking sites within lesson times
Staff need to use social networking in a way that does not conflict with the GTC code of conduct , TDA Core Standards or Personnel handbook
Staff should review and adjust their privacy settings to give them the appropriate level of privacy

Staff communication

Staff should only communicate with pupils and parents through official channels. These channels include:

- Post on school letter headed paper
- School telephone system
- School e-mail system
- Dojo behaviour system

The following are excluded from the official channels:

- Social networking sites
- Gaming sites

- Chatrooms
- Personal mobile phones
- Personal e-mail addresses
- Personal video conferencing solutions (eg Skype)

Education

Pupils

The pupils will receive two blocks of e-safety teaching throughout the year. One session will take place in the Autumn term and another in the Spring term for E-safety week. We use NSPCC Internet Legends to support E Safety. We will share information with parents.

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive e-safety education programme that is fully embedded for all children , in all aspects of the curriculum, in all years.
b). Regularly auditing, review and revision of the ICT curriculum
c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
c). The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour
d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

a). A planned programme of formal e-safety training is made available to all staff
b). E-safety training is an integral part of Child Protection / Safeguarding
training and vice versa
c). An audit of e-safety training needs is carried out regularly and is
addressed
d). All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
e). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
f). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
g). The school takes every opportunity to research and understand good practice that is taking place in other schools
h). Governors are offered the opportunity to undertake training.

Parents and the wider community

Parents are made aware of e-safety resources available for them and will be given key information during the Autumn term. During e-safety week in February parents will be signposted to key documents that will be uploaded onto dojo. Interland an internet safety game will be shared with the parents to promote being safe online.

Monitoring and reporting

a). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

b). The records are reviewed / audited and reported to:

- the school's senior leaders
- STG
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

ICT Acceptable Use Policy (AUP) KS1

Pupil Agreement / ESafety Rules

This is how I stay safe when I use computers:

I will ask a teacher if I want to use a Chrome Book / Ipad.

I will not play apps or look at websites that are too old for me.

I will only use activities that a teacher has told or allowed me to use.

I will send messages that are polite.

I will only email people I know.

I will not tell people about myself online (I will not tell them my name or anything about my home).

I will not upload pictures of myself without asking a teacher.

I will take care of the computers and other equipment.

I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a Chrome Book / Ipad.

..... [Print child's name] agrees to follow the ESafety rules and to support the safe use of ICT at Burford Primary School.

Signed.....

Class .....

Date.....

ICT Acceptable Use Policy (AUP) KS2

Pupil Agreement / eSafety Rules

- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately look for, or access inappropriate websites or apps. I will consider the age-appropriate certificate when playing games or viewing videos.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not allow myself to get involved in incidents of cyber-bullying either at school or home via apps or websites such as What's App, Snapchat or Facebook
- I will not give out my own, or others' details such as names, phone numbers or home addresses or photos when using devices at school or home.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network or at home without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I will not use my mobile phone in school for any reason. If I do bring my phone to school with me I will follow the school's mobile phone policy.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

..... [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at Burford Primary School.

Child's Name (Signature) .....

Class ..... Date.....

ICT Acceptable Use Policy for any adult working with learners

eSafety Rules

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- inappropriate images
- promoting discrimination of any kind
- promoting violence or bullying
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling

- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

Burford CE Primary School

Parent / guardian name:……..
Pupil name: …….
Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

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

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent's signature:…… **Date:**…….

Appendix 3 – School audit

Audit

The self-audit in should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Shropshire guidance? Yes/No

Date of latest update (at least annual): _____

The Leadership team member responsible for e-safety is: _____

The governor responsible for e-Safety is: _____

The designated member of staff for child protection is: _____

The e-Safety subject lead is: _____

The e-Safety Policy was approved by the Governors on _____

The policy is available for staff at: _____

The policy is available for parents/carers at: _____

Appendix 4 – Photo/video consent

Photo/Video Consent Form

School Name**: BURFORD C.E. PRIMARY SCHOOL**

Name of child: _____

Class:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, in school work books, or on all four. They may also be used by the local newspapers.

To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

1. May we use your child's image in our printed promotional publications? Yes / No

2. May we use your child's image on the school website/SLG? Yes / No

3. May we record your child's image on our promotional videos? Yes / No

4. May we use your child's image in the local press? Yes / No

5. May we use your child's image in the children's class work books? Yes / No

Signature:…… Date: …….

Your name (in block capitals):