Burrough Green CE Primary School

ICT ACCEPTABLE USE POLICY

Incorporating Use of Images Policy

and Mobile Phone Policy

Summer 2018

Introduction

Information and communication technologies are indispensable tools for school staff and pupils, however they also pose significant risks for the school. The most serious risk to pupils using the internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being disclosed online. Pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm. The risk to children may not be immediate, since there can be a long period of building-up a relationship, known as the 'grooming process.'

This Acceptable Use Policy (AUP), reviewed every three years, provides adults at Burrough Green CE School with guidance on how to make the best use of these technologies whilst limiting potential dangers. No adult working in school should use the School's internet or e-mail without being familiar with this Acceptable Use Policy. The school will encourage parents to be aware the risks of internet and e-mail use in order that they can take precautions at home.

All Internet access is filtered through a proxy server to screen out undesirable sites at source, however occasionally unsuitable sites can slip through. Pupils are taught procedures to follow if an unsafe site is located during lesson time and staff make a note of the web address. This is reported to the ICT Leader immediately who will arrange for an email to be sent to the ICT service informing them of the site so that future access can be prevented ict.helpline@cambridgeshire.gov.uk

Pupil Use of the School's Internet and E-mail Services

Teachers must:

- link the teaching of internet and e-mail based-skills to the curriculum
- use sites saved to *Favourites* whenever possible
- use sites known to be child-safe whenever possible
- check any open searches they intend to ask pupils to do in advance to limit risks – particularly for an 'image' search as pictures are not always easy to filter
- teach pupils not to share any personal information such as name or address at any time when e-mailing an unknown person or organisation, or using the internet (at home or school) and the reasons why this could be unsafe
- teach pupils what to do if they accidentally find an unsafe site while using the internet
- teach pupils to speak to their teacher, parents or carers if they feel unsure or unsafe
- teach children to involve teachers, parents and carers whenever they are communicating with people that they do not know
- display the pupil acceptable use statements in the classroom (Appendix 1)

- teach pupils to use the internet responsibly and to speak to their teacher, parents or carers if they feel unsure or unsafe
- teach pupils that web sources could be unreliable and inaccurate and to check their information against other sources and not to rely on just one information source
- supervise pupil use of the internet and e-mail

How will the policy be introduced to pupils?

Pupils will need to be reminded regularly about the pupil acceptable use statements. This will be done in lesson time when the need arises. Rules for Internet access will also be posted in the classroom and on the front of laptop trolley.

Staff Use of the School's Internet Service

The school wishes to encourage the use of e-mail and internet by staff in support of their work and the use of these facilities should be appropriate to the work, standards and ethos of the school.

The use of the school's internet and e-mail systems is not provided as a right to any of their users. They may be withdrawn from any user adult or pupil who does not conform to this Acceptable Use Policy. The school is responsible for authorising any user of its internet or e-mail facilities, and may monitor their use.

Any member of staff who commits a serious offence in the use of the schools internet service may be subject to the school's staff disciplinary procedures.

Any user, adult or pupil, who breaks the law in respect of using the schools internet service will be reported to the police.

Staff must not upload images to websites without complying with the School's guidance on images loaded to the internet.

Staff must work within central hosting if the document contains any personal information.

Staff must lock their computer when it is unattended.

Staff must not share, make obvious or leave in an insecure place any passwords associated with using the internet, e-mail and computer system.

Staff or administrative users should be mindful to protect the school from computer virus attack or technical disruption when downloading from the internet any programs or executable files other than by agreement with the schools ICT subject leader.

Staff must never provide personal details or contact details of their own, or any other person, to internet sites including weblogs, forums or chat rooms. Exceptions should be checked with the Headteacher. At all times comply with the GDPR.

Staff must report any unacceptable sites or material immediately to the Headteacher, ICT Leader or the Education ICT Service Helpline – 0300 300 000. Action can then be taken to block the site or material.

Staff or approved adult school users should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet.

Staff using a school laptop or other device off the school site, at home or elsewhere, will still have to abide by the school internet Acceptable Use Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the *Computer Misuse Act (1990)*.

Staff should not allow family or friends to use their laptop under any circumstances, and staff must ensure that passwords that enable use of the equipment must be kept securely and not divulged.

School laptops remain the property of the school and are provided solely for the purpose of assisting staff in fulfilling their professional duties. They should not, therefore, be used to store personal information, such as family photographs.

Staff will at all times work to maximise the safety of pupils within their care in their use of the internet.

Colleagues will be aware of the ethos, standards, equalities and ethnic mix of the school and will not access any internet material, or work with the internet, in any way that infringes or offends these.

Virus protection software is installed and updated regularly using Sophos Anti Virus as recommended by the CCC ICT Service.

Staff use of the School's E-mail Service

Use of the School e-mail service must conform with the Council e-mail code of practice at all times which is based upon the Governments Safe Working Practices guidelines and existing network security guidance as published by the Local Authority and detailed on the front cover of this policy. Guidance on good e-mail pro-active can be found here: https://theictservice.org.uk/service/house-keeping-for-effective-mailbox-management/

The content of e-mails or an attachments must be treated in the same way as any other paper based letter or document. GDPR apply equally to electronic messages and documents

as they do to paper documents, as do the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination. Remember it is easy for your e-mail to be passed on electronically to others should any recipient decide to do so.

Staff should make sure that the 'subject' field of any e-mail that they send is meaningful and representative of the message it contains.

The schools e-mail system should not be used by any user (adult or pupil) for the sending of personal mail unconnected with school work or activity unless specifically approved by the Headteacher, or senior member of staff.

Staff should remember that sending an e-mail from the school e-mail account is similar to sending a letter on school letter headed paper, and must not in any way bring discredit or embarrassment to the school or local authority.

Any e-mail received by a member of staff, which is regarded as illegal or offensive, should be reported to the Headteacher immediately. Similarly, any e-mail sent or received by a student, which is regarded as illegal or offensive, should be reported to the Headteacher immediately.

To safeguard against computer viruses, staff must not open external e-mails or an e-mail attachment that looks in any way suspicious. These should be reported it to the school's ICT leader for checking.

Staff should never make changes to someone else's e-mail and then pass it on without making it clear that changes have been made.

Staff must not copy images or any other material for use in e-mails or attachments that infringe the copyright law.

Never give your Portal/e-mail password to anyone else.

Emails should only be printed if it is absolutely necessary to do so.

Staff using social networking sites should not add parents of school children at Burrough Green CE School, current or ex-pupils onto their 'site' as friends. This avoids a potential of 'conflict of interest' situation and maintains the parent/teacher trust and respect.

Staff using social networking sites must not bring themselves, or the school, into disrepute. Simple steps can be taken to ensure this by reviewing privacy settings, and ensuring images and/or messages are discrete, and do not breach confidentiality rules.

Chain letter emails should not be opened or forwarded.

Unless authorised to do so, staff must not send an e-mail to any supplier that could be interpreted as creating a contract in any way. In general, staff should not use e-mails for contractual purposes. NOTE: within the law, a user could send an e-mail containing wording which may form a legally binding contract with a supplier.

Staff must never open an attached program file with a file extension of “exe”, “com” or “bat” sent to you with an e-mail unless you are absolutely certain that it has come from a trusted source. All such files must be thoroughly virus checked before they are opened.

Reading other people’s email is not permitted.

The E-safety Leader is supported by the Head Teacher.

Use of Images Policy

The school believes that the taking and use of photos and videos (hereafter referred to as images) is a very positive part of recording school life and the individual achievements of pupils. The school website and twitter feed increases pupil self-esteem and provides information to parents and the community. However, a parent may have genuine reasons for not wanting their child to appear in a photo or video e.g. personal safety or concern about the potential manipulation/use of images. The purpose of this policy is to establish clear guidelines for staff, volunteers and parents regarding the use of images.

Images taken of children during school or at events fall into two categories:

- Images for school use which are subject to the GDPR (2018). These images used by the school for e.g. the prospectus, marketing, website, twitter, displays, recording learning etc. and require parental consent. (Further information can be found in the school’s Privacy Notice)

- Images taken for personal use, e.g. by parents at school events. These are not subject to the GDPR (2018) and must not be used for commercial purposes, used by the Press, on social media or other websites, or in any other way be put into the public domain. Any person taking images that is not known to the school will be asked to produce identification and the reason established for the interest in the event.

As each pupil joins the school, a use of images consent form is given to all parents. If parents decline consent, this is communicated to staff to ensure that this request for exclusion is adhered to within the capabilities of the school. It is school policy that images are never accompanied by names. Care is also taken to ensure that the filename of a

photograph (eg. johnsmith.jpg) does not inadvertently identify a child. Accompanying text will also not name any children photographed.

Staff must not use their own cameras, mobile phones or computers to capture or share images.

All photographs of children will be taken in such a way as to ensure that the individual identity of a child is protected and care is taken in choosing suitable activities to be photographed e.g. children changing must not be photographed/recorded. If any image is accidentally taken that is then deemed unsuitable it will be destroyed in an appropriate confidential manner (e.g. shredded/deleted).

We encourage press coverage where this builds confidence, pupil esteem or positive images in the community but will refuse if we feel it is not in the best interests of the school or will breach privacy. Consent is requested when children enter school via the signed consent form. We do not allow images to be taken by journalists/others who attend the school without invitation.

Mobile Phone Policy

In addition to the above the following guidelines for use of mobiles phones in school must be followed:

- Pupils should not bring mobile phones to school
- Personal staff phones should be switched off in school, or left securely in a locker in the staff room (except when used as the emergency contact during swimming lessons, when they must only be used to make emergency 999 calls)
- If communicating officially with parents via a mobile phone a school mobile should be used
- A school mobile should always be taken on educational visits in case of emergencies
- When communicating with parents in any way via a mobile phone staff should abide by the policy requirements laid out below.
- Mobile phones must not be used to photograph images of pupils attending Burrough Green CE Primary School. Volunteers or work experience students must not take or store images of children.

Informing parents / carers

Parents' attention will be drawn to this AUP when their child joins the school and when the policy is updated and it is available on the school's website. Advice that accords with acceptable and responsible Internet use by students at home will be made available to parents. Safety issues will be handled sensitively.

If parents take images e.g. photos or videos of events at school that include other children they must not share it e.g. on a social networking site or their own website.

The school will obtain parental consent for use of images. (Appendix 3)

Insurance

If teachers choose to take their school allocated laptops home they will be covered whilst at home or during transit by school insurance. School laptops must not be left unattended in cars.

Reviewed Summer 2018

AUP Policy ratified Summer 2018

To be reviewed Summer 2021

APPENDIX 2

I confirm I have read the schools ICT and AUP Policy and agree to follow the code of conduct as outlined.

Name (BLOCK CAPITALS) _____

Signature _____

Date _____

APPENDIX 3

Internet/Media Permission Form
Childcare Provider: Burrough Green CE Primary School

I am the parent/legal guardian of the child(ren) named below and I give permission for my child(ren) to be photographed, videotaped, or to use the internet whilst in the care of the provider named above for the following purposes (please tick all that apply):

For use in school –

	Photo albums
	Displays
	Staff course work and in children's books
	Internet research – will be supervised at all times
	Website – children's work will be identified using first names only and photographs of children will not be named.
	Twitter – to provide an up to date series of images about school life. Children photographed will not be named.

For external use –

	Printed media e.g. local newspapers. Groups of less than 8 children will be named. This is a media stipulation.

Child's/ren's name/s (BLOCK CAPITAL)
Parent's name (BLOCK CAPITAL)
Address:
Parent's signature: Date:

Appendix 1:

Acceptable Use Statements for Young People

My e-Safety Agreement – KS2

This is my agreement for using the Internet safely and responsibly.

- I will use the Internet to help me learn.
- I will learn how to use the Internet safely and responsibly.
- I will only send email messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to put online photographs or video clips without permission and I will never use my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the Internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my Internet in a safe and responsible way.

Signed..... Dated.....

Appendix 3:

Acceptable Use Policy for Young People

My e-Safety Agreement – Years R, 1 & 2

This is my agreement for using the Internet safely and responsibly.

- I will only go on the internet if an adult lets me.
- I will use the Internet to help me learn.
- I will not talk or type messages to people I don't know.
- I will always be polite and friendly to people on the internet.
- I will never tell anyone on the internet anything about me, except my first name, unless my teacher says I can.
- I will tell a teacher if I see or hear something I don't like.

Signed..... Dated.....

Name.....(Printed)