Baston CE Primary School

ESafety Policy

Table of Contents

1. Introduction

1.1 The internet can potentially give children access to material of an unsuitable nature and could also lead to children receiving unsuitable communications through electronic mail, social media or chat rooms. It is the school's policy to make every reasonable effort to protect pupils from such material but also to make them aware of the potential dangers at an appropriate level for their age.

2. Policy Governance

Development, Monitoring and Review of this Policy

2.1 This e-safety policy has been developed by the Pupil Support Community and Leadership (PSCL) Committee made up of:

Position	Name(s)
School E-Safety Coordinator / Officer	R Mills
Headteacher	R Mills
ICT Technical staff	ARK IT Solutions Ltd
Governors	S Gledhill

Schedule for Review

This e-safety policy was approved by the PSCL Committee on	25th February 2020
The implementation of this e-safety policy will be monitored by the Headteacher	R Mills
Monitoring will take place at regular intervals:	Annually
The E-Safety 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. The next anticipated review date will be	February 2021
Should serious e-safety incidents take place, the following external persons / agencies should be informed	Lincolnshire Safeguarding Children Partnership

3. Scope of the Policy

3.1 This policy applies to all members of the school community (including staff, pupils, governors volunteers, parents/carers, visitors) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

4. Roles and Responsibilities

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

4.1 Governors

Are responsible for:

- the approval of the E-Safety Policy and for monitoring its implementation via the Safeguarding governor of the school.

4.2 Headteacher and Senior Leaders

Are responsible for:

- ensuring the safety (including e-safety) of members of the school community
- being aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

4.3 E-Safety Leader

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/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
- coordinating training and signposts advice for staff
- receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reporting regularly to the governing body via meetings with safeguarding governor

4.4 Technical staff

ARK IT Solutions is 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 Lincolnshire City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

4.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the headteacher for investigation/action/sanction

4.6 Designated person for child protection

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data

- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

4.7 Pupils

- are responsible for using the school ICT systems and mobile technologies in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

4.8 Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and website about e-safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

5. E-Safety Education and Training

5.1 Education – pupils

E-Safety education will be provided in the following ways:

- a planned e-safety programme will be provided as part of ICT/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- key e-safety messages will be reinforced as part of a planned programme of workshops
- pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

5.2 Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the appraisal process.
- all new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy.

6. Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods. Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff and other adults				Pupils			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed ONLY with staff permission	Not allowed
User Actions	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to school	☑						⚠	
Use of mobile phones in lessons				☒				☒
Use of mobile phones in social time		⚠						☒
Taking photos on personal mobile phones or other camera devices				☒				☒
Use of personal hand held devices eg PDAs, PSPs		⚠						☒
Use of personal email addresses in school, or on school network				☒				☒
Use of school email for personal emails				☒				☒
Use of chat rooms / facilities				☒				☒
Use of instant messaging		⚠						☒
Use of social networking sites				☒				☒
Use of blogs				☒				☒

⚠ This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff and other adults**	**Pupils**
Mobile phones may be brought to school		When a written request by a parent/carer has been authorised by the Headteacher for child security purposes
Use of mobile phones in lessons	Never	Never
Use of mobile phones in social time	During break and lunchtime in staff room or offices	Never
Taking photos on personal mobile phones or other camera devices	Never	Never
Use of personal hand held devices e.g. PDAs, PSPs	During break and lunchtime in staff room or offices	Never
Use of personal email addresses in school, or on school network	During break and lunchtime in staff room or offices	Never
Use of school email for personal emails	Never	Never
Use of chat rooms / facilities	Never	Never
Use of instant messaging	During break and lunchtime in staff room or offices	Never
Use of social networking sites	Never	Never
Use of blogs	Never	Never

7. Unsuitable/inappropriate activities

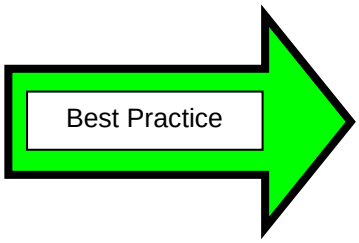
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑	⚠	⚠	☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the *Obscene Publications Act* in the UK					☒
criminally racist material in UK					☒
pornography				☒	
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
promotion of racial or religious hatred					☒
threatening behaviour, including promotion of physical violence or mental harm					☒
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☒	
using school systems to run a private business				☒	
use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LA and/or the school				☒	
uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					☒
revealing or publicising confidential or proprietary information (for example: financial/personal information, databases, computer/network access codes and passwords)					☒
creating or propagating computer viruses or other harmful files					☒
carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				☒	
on-line gaming (educational)			⚠		
on-line gaming (non-educational)				☒	
on-line gambling				☒	
on-line shopping/commerce			⚠		
file sharing			⚠		
use of social networking sites			⚠		

use of video broadcasting for example: YouTube					
accessing the internet for personal or social use (for example: online shopping)					
using external data storage devices (for example: USB) that have not been encrypted, password protected and checked for viruses					

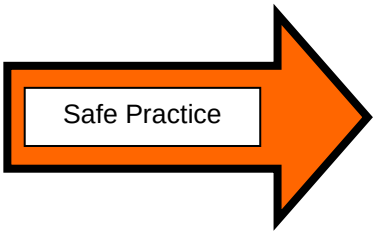
8. Good practice guidelines

Email

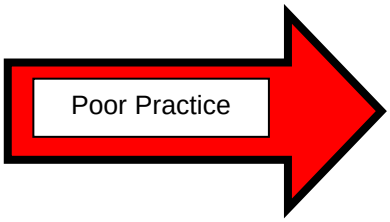


☑ DO

Staff and students/pupils should only use their school email account to communicate with each other



Check the school e-safety policy regarding use of your school email or the internet for personal use for example: shopping



☒ DO NOT

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

9. Images, photographs and videos

Best Practice

☑ DO

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe Practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/Chair of Governors knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor Practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/Chair of Governors knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

10. Internet

Best Practice

☑ DO

Understand how to search safely online and how to report inappropriate content.

Safe Practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

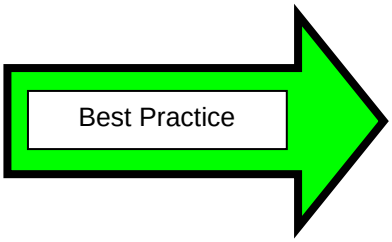
Poor Practice

☒ DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

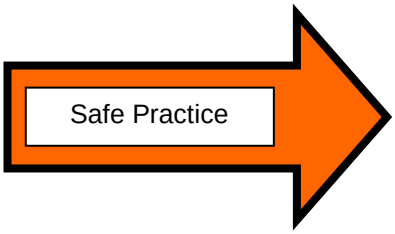
11. Mobile phones



☑ DO

Staff:

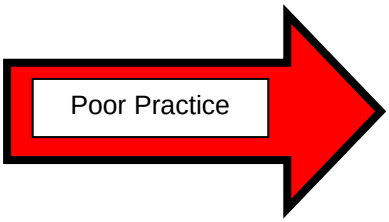
- if you need to use a mobile phone while on school business (visits etcetera), make sure it is the phone that is registered against your name on Staff Contact list
- make sure you know about inbuilt software/ facilities and switch off if appropriate



Check the e-safety policy for any instances where using personal phones may be allowed.

Staff:

- make sure you know how to employ safety measures like concealing your number by placing 141 in front of the required number



☒ DO NOT

Staff:

- don't use your own phone without the Headteacher/Chair of Governors knowledge or permission
- don't retain service pupil/parental contact details for your personal use

12. Social networking (for example: Facebook/Twitter)

Best Practice

☑ DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe Practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor Practice

☒ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- don't accept pupils or their parents as friends on your personal profile
- don't accept ex-pupils users as friends
- don't write inappropriate or indiscrete posts about colleagues, pupils or their parents

13. Webcams

Best Practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/Chair of Governors knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Safe Practice

Poor Practice

☒ **DO NOT**

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/Chair of Governors knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

14. Incident Management

Incidents (pupils):	Refer to class teacher	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction for example: exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		☑			☑	☑	☑	
Unauthorised use of non-educational sites during lessons	☑	☑		☑	☑	☑	☑	
Unauthorised use of mobile phone/digital camera / other handheld device	☑	☑			☑			
Unauthorised use of social networking/ instant messaging/personal email	☑	☑			☑	☑	☑	
Unauthorised downloading or uploading of files	☑	☑		☑	☑	☑	☑	
Allowing others to access school network by sharing username and passwords	☑	☑			☑	☑	☑	
Attempting to access or accessing the school network, using another pupil's account	☑	☑		☑	☑	☑	☑	
Attempting to access or accessing the school network, using the account of a member of staff	☑	☑		☑	☑	☑	☑	
Corrupting or destroying the data of other users	☑	☑			☑	☑	☑	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑	☑			☑	☑	☑	
Continued infringements of the above, following previous warnings or sanctions	☑	☑			☑	☑	☑	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☑	☑		☑	☑	☑	☑	
Using proxy sites or other means to subvert the school's filtering system	☑	☑		☑	☑	☑	☑	
Accidentally accessing offensive or pornographic material and failing to report the incident	☑	☑		☑	☑	☑	☑	
Deliberately accessing or trying to access offensive or pornography	☑	☑		☑	☑	☑	☑	
Receipt or transmission of material that infringes the copyright of another person or infringes the *Data Protection Act*	☑	☑		☑	☑	☑	☑	

Incidents (staff and volunteers):	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)	☑	☑	☑	☑	☑	Disciplinary, Ban from school site
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	☑		☑	☑	☑	
Unauthorised downloading or uploading of files	☑		☑	☑	☑	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	☑	☑ (vols)	☑	☑	☑	
Careless use of personal data for example; holding or transferring data in an insecure manner	☑		☑		☑	
Deliberate actions to breach data protection or network security rules	☑	☑ (vols)	☑	☑	☑	Disciplinary Ban from school site
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	☑	☑ (vols)	☑	☑	☑	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑	☑ (vols)		☑	☑	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	☑	☑ (vols)	☑	☑	☑	
Actions which could compromise the staff member's professional standing	☑				☑	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☑	☑ (vols)	☑	☑	☑	Disciplinary Ban from school site
Using proxy sites or other means to subvert the school's filtering system	☑		☑	☑	☑	
Accidentally accessing offensive or pornographic material and failing to report the incident	☑		☑		v	
Deliberately accessing or trying to access offensive or pornographic material	☑	☑	☑	☑	☑	Disciplinary Ban from school site
Breaching copyright or licensing regulations	☑				☑	
Continued infringements of the above, following previous warnings or sanctions	☑					

Appendix 1 – Pupil Acceptable Use Policy

1. Pupil Acceptable Use Policy

1.1 Pupil Acceptable Use Policy Agreement

This Pupil Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.

☑ I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- 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
- not bring or use any personal handheld/external devices (mobile phones/USB devices, for example) in school
- immediately report any damage or faults involving equipment or software, however this may have happened
- not use chat and social networking sites

☒ I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- 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
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings

2. Pupil Acceptable Use Agreement Form

2.1 This form relates to the pupil Acceptable Use Policy (AUP), to which it will be attached.

2.2 I understand that using the computer network at Baston CE Primary School is a privilege which could be taken away from me.

2.3 When using the computers I will:

- always behave sensibly, respecting other members of the school
- only log in using my own username
- keep my password secret, if I have one
- never access or distribute any material on the network which may upset/be considered offensive by others
- close down any upsetting/offensive material which has been accessed by mistake and report it to my teacher
- **be polite at all times**, both to those around me and those I contact through the network
- **report any upsetting/offensive messages I receive through the network to my teacher or Headteacher**
- not waste my time playing non-educational games
- not download any games or other programs without the permission of my teacher
- **never enter my address, telephone number, photograph or any other details about me or anyone else**
- only enter the school address after I have got permission from my teacher, and will never enter the school telephone number behave sensibly when using computers at school, especially when I am on the internet
- tell my teacher if I find something upsetting on the internet
- never give away my address, telephone number, photograph or any other details about me or anyone else when I am working on the computer

3. If I break any of these rules I will report it to my teacher as soon as possible and realise that I may be punished, but that my honesty will be recognised.

Name of Child/Pupil:		
Signed (Student/Pupil):		Date:

I acknowledge the Acceptable Use (eSafety) Policy and the Pupil's Acceptable Use Agreement and support the school in its efforts to keep children safe when using technology and the internet as well as making them aware of the dangers.

Signed (Parent/Carer):		Date:

Appendix 2 – Staff, Volunteer, Community User AUP

1. Staff, Volunteer and Community User Acceptable Use Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

2. Acceptable Use Policy Agreement

2.1 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 recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (for example: laptops, email, school website etc) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (for example: on the school website) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- when I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses

- I will not use personal email addresses on the school ICT systems
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 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 will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies and I am specifically authorised/requested to do so
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos)

2. Staff, Volunteer and Community User Acceptable Use Agreement Form

2.1 This form relates to the Acceptable Use Policy (AUP), to which it will be attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

3. I have read and understood the School's E-safety Policy

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:	
Position:	
Signed:	
Date:	

Appendix 3 – Use of Images Consent Form

1. Use of Digital / Video Images

1.1 The use of digital/video images plays an important part in learning activities. Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to give or withhold their permission to allow the school to take and use images of their children via the pupil details form. The information provided will be stored by the school via Integris in accordance with our data protection policy.

This update form is requested on an annual basis and must be returned before digital/video images of children are taken.

Baston CE Primary School Acceptable Use Agreement/Code of Conduct:
Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher, depending on the seriousness of the offence; investigation by the head teacher/ governors, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- I will only use the school's email / Internet / Learning Platforms and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware or software without seeking permission from the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……Date ……

Full Name ……..... (printed) Job title . . . . . .