Computing and Online Safety Policy

RATIFICATION: Autumn 2025
DATE OF NEXT REVIEW: Autumn 2026
REVIEWED BY: Executive Headteacher
APPROVED BY: Local Governing Body

Responsibilities

The member of SLT responsible for e-safety is	P O'Malley
The Governor responsible for safeguarding/e-safety is	Rev Jon Aldwinckle
The e-Safety Co-ordinator is	P O'Malley

The e-Safety Co-ordinator is responsible for developing the e-safety curriculum (through both computing and, where necessary, PSHE), 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 school community. They may also be required to deliver workshops for parents.

Alveley Primary School is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective way to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure and the safety of its users is the responsibility of all staff.

Acceptable Use Policies (AUPs)

This policy relates to any ICT use in school or on school business. It relates to all school equipment and all school initiated communication systems - this includes all work within the cloud. As such the policy provides guidance for our working and private practice both within and outside of school. In particular this policy extends to out of school use including:

- Our email system from any location
- Use of school equipment in and out of school
- The access to the school's Office 365 applications via the internet.

All stakeholders must be aware that any infringement of current legislation, ie Data Protection Act 1998 and General Data Protection Regulations (GDPR), Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988, will be regarded as a breach of school policy and may be treated as gross misconduct. In some circumstances such a breach may also be a criminal offence.

ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and, as such, all users have a personal responsibility for ICT security and safety both inside and outside of school.

Ensure that equipment is sited so as to avoid environmental risks, eg dust, heat. This also applies to official equipment used at home. Ensure that items are kept securely following reasonable precautions to prevent loss, damage or theft.

All members of the school community should agree to an Acceptable Use Policy (AUP) that is appropriate to their age and role. AUPs used can be found in **appendix 1.**

AUPs will be reviewed periodically. All AUPs will be stored centrally in case of breaches of the e-safety policy.
E-safety forms a part of all computing teaching and the AUP will form part of this.

Email and Internet use

All internet activity should be appropriate to the function of educating, or supporting the education of children, young people and adult learners in school related matters. Personal email use may occasionally be used, however this use should be infrequent and marked 'personal.' No school related business should be communicated through personal email. The content of all email accessed in school or generated by the school's email system may be checked under the direction of the Head Teacher.

All staff and pupil internet usage is monitored. This may be logged and kept for an appropriate length of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are only available to authorised personnel and kept for no longer than necessary in line with the current data protection policy.

Users must respect the work of others which might be stored in common areas.

The use of public chat rooms and social media sites/applications is not allowed on school equipment or via Personal Electronic Devices (PEDs) whilst on the premises (other than in designated staff areas, such as the staff room). However, professional on-line forum may be appropriately used for professional business and/or professional development. Posting anonymous messages and forwarding chain letters is forbidden. Comments or information which harms the school or school members may not be posted or distributed.

All members of the school community are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Photographs and Video

Under GDPR regulations photos are classed as personal data. As a school we must have a lawful basis to use these. In most cases this is part of our public task of education e.g. photos/videos needed for exam courses or to support teaching and learning.

However, where photos are required for other purposes (e.g. school marketing) consent is the other lawful basis that can be used. When this is the case and in using all photos pupil records should be checked.

Staff must be fully aware of the consent form responses from parents when considering use of images. The consent form is part of the school registration form and all data can be accessed in SIMS **(appendix 2).**

Pupils should not bring to school any PED that has the capacity to take photographs, videos or audio, or be able to communicate externally via. messaging or call services. In the rare instances where a pupil needs to (for example to measure insulin levels as part of a diabetes care plan), this will be fully risk assessed and written consent given by the Headteacher. Likewise, Year 6 pupils may bring a phone into school if both school and parents have agreed to them walking home by themselves. Rules around this are covered in our Mobile Phone Policy, which all pupils and parents must sign prior to bringing a device into school.

It is the member of staff's responsibility to ensure that this is checked and the schools to review this annually.

Best practice suggests that staff should only use a school owned device to capture images and that images should be held securely on the schools One Drive account and be removed from any storage devices as soon as possible.

Photos taken by the school are subject to the Data Protection Act and General Data Protection Regulations (GDPR). With any displays of personal information safeguarding risks should be evaluated as well.

Photos and videos taken by parents/carers.

Parents and carers are not permitted to take photos/videos of children in school events unless they are given specific instructions from a member of the SLT. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

Mobile phones and other Personal Electronic Devices (PEDs)
Staff mobile phones should be switched to silent whilst on the school premises and remain out of sight and not used, unless in a designated staff area such as the staff room.

Visitors to school should ensure that mobile phones/ other devices are switched off and handed in to the office. The only exception being when their phone is an integral part of why they are in school. An example may be somebody conducting a fire safety audit, who needs to photograph infringements, or improvements since a previous visit.

Security and passwords

Staff are informed that they must change passwords regularly. Best practice indicates that passwords should be changed at least termly. Passwords should not be re-used and should be made up of a minimum of 8 alphanumeric characters. They should not be obvious or guessable. Access should only be made to school systems via the authorised account / password, which should not be made available to any other person.

Passwords should be changed immediately if the use believes or suspects that their account has been compromised.

When accessing on-line cloud services such as Office 365 (Files and email) staff should be using school equipment that is only accessible to them. School devices are only for the member of staff that has been allocated the equipment.

If using personal computers, PEDs or mobile phones staff are required to ensure that these are password protected and that they fully logout of any work related systems. If this cannot be guaranteed then personal devices should not be linked to work accounts.

Best practice would suggest that software is not used to link multiple accounts e.g. personal and work emails picked up together in Outlook or alternative providers.

Staff & students must always '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'). Personal data such as SIMs should never be shown through a data projector.

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

Data storage

Staff are instructed to only use encrypted USB drives or hard drives in school. Best practice would suggest uploading files into the schools cloud storage (One Drive). If staff are backing up work it should be on an encrypted hard drive using Bit-locker software. Staff are advised not to save work directly to the computer in case of theft.

Reporting

All breaches of the e-safety policy need to be recorded in SIMS as part of the schools behaviour management sanctions. These incidents will be collated by the e-Safety Co-ordinator.

Incidents which may lead to child protection issues need to be passed on to the designated safeguarding lead immediately – it is their responsibility to decide on appropriate action.

Incidents which are not child protection issues but may require SLT intervention (eg cyberbullying) should be reported to the Headteacher as soon as possible.

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 and safe guarding guidelines. If necessary the Local Authority Designated Officer (LADO) should be informed.

Evidence of incidents must be preserved and retained.

The curriculum and assembly programme will cover how pupils should report incidents (eg Child Exploitation and Online Protection (CEOP) button, trusted adult, Childline). The school's website is also regularly reviewed to provide information to parents regarding e-safety.

Infringements and sanctions

Whenever a pupil infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher. Any pupil in breach of the policy faces the full range of school sanctions including exclusion.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and collect evidence, the Trust's Human Resources team and Telford & Wrekin IT services.

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 – e.g. class commendation for good research skills, certificates for being good cyber citizens etc.

The member of the SLT should endeavour to reward any student for outstanding and/or responsible use of ICT in line with the school's rewards policy.

Social networking

Pupils and staff are not permitted to use social networking sites within school, except in designated staff areas, such as the staff room.

Best practice would suggest that staff who use social networking outside of school should never comment on school related business and ensure that privacy settings are set to secure or private.

For teachers, using social media has many benefits in terms of professional networking to improve and support teaching and learning. However teachers must be aware of the risks. As per the NASUWT recommended guidance the school policy is:

- Do not post anything that could be construed as defamatory or discriminatory against others or the school. Any post can be potentially quoted by the media
- Do not make or accept friend requests by pupils (current or past) or parents.
- Ensure your privacy settings are adequate. You can determine who sees your posts and most importantly, ensure that you get to approve any pictures in which you may be tagged before the picture is published. You can also disable your profile from certain search engines.
- Any social media accounts should not be linked or registered using your work email address.
- When joining or being added to any groups, always check whether it is Public, Closed (where anyone can see the members of the group but not the discussion) or Secret (where neither the members or the discussion are visible)
- Sharing, forwarding or 're-tweeting' can be viewed as a sign of endorsement. This may be inappropriate in some circumstances.

These guidelines are designed to protect all users of ICT. However, if these rules prevent you from doing your job then permission should be sought from the headteacher in writing. This also includes permission to set up any social media accounts related to school.

Physical security of equipment

Staff are issued with computer resources based upon their role. All allocated resource should be kept in good working order. Staff must ensure that equipment is looked after. Any accidental damage must be reported to the network manager immediately and where possible to your house insurance.

If taking resources off site they should only transported in the boot of a car (but not left in boot when parked) and safely secured at home.

Any ICT resources are allocated for business use and must not be used by non-Trust employees.

Staff will be requested to sign for all equipment as part of staff induction.

Software

Staff must not add software onto the school system without consulting the ICT Network technician.

Any software that requires personal data of students or staff should not be purchased prior to checking with the Data Protection Officer to ensure GDPR regulations are followed. If guarantees cannot be made then the software will not be used on the schools IT system.

Staff must ensure that all software is updated as per the requests of the network technician to ensure security of the system.

Email Policy

This guidance aims to enhance the use of email as part of the portfolio of communication media and develop good practice in the use of email as a medium of communication.

Sending emails

Before sending emails consider:

- The maintenance of the highest professional standards – think about how they could be read.
- Whether email is the correct medium for communication.
- To whom should the email be sent, consider expected communication style.
- Only copy in people who have an immediate need for the information. Whole school or All Staff emails should be avoided where possible.
- Please consider the sensitivity of the email topic. Best practice would be to upload the information to shared areas on One Drive/ SharePoint or to password protect confidential information prior to attachment.
- The length of the email, avoid long detailed emails.
- Always check the recipients of your email – Best practice is to write the email first and then add the email address in. Staff should also take care in using the Reply all function.

In the case that emails are sent to the wrong address that contain personal information Staff must attempt to recall the email using the recall tool. If this is unsuccessful as part of GDPR the Schools data protection officer must be informed. This is a legal requirement.

Always read and check your email before sending.

Receiving and Managing emails

- Staff should become 'responsible communicators' i.e. they should check their emails at the start of each day.
- Consider whether they need you to respond, retain print and/or delete.

• If they require retention, place emails and attachments in folders. Emails should not be used as a storage area for information. School emails will automatically be deleted from the system in line with the schools data retention policy.
• If they require response consider carefully the use of the “reply to all” button.
• Delete unwanted emails promptly.
• Protect yourself from viruses when emailing from home or from email addresses that are unrecognised and that contain attachments.

Sensitive Information

• Emails are the electronic equivalent of a postcard. Anyone can read the content along the delivery path. Sensitive information should be sent by post or via a secure transfer system.
• Child Protection issues should not be reported via email.
• Never email in haste, consider the facts and consequences of the message.
• Be professional and careful about what you say about others, as email is easily forwarded. Only put in writing what you would say to someone’s face.
• Be aware of copyright and libel issues e.g. when sending scanned text, pictures or information downloaded from the internet.
• An email can be contractually binding. Therefore care should be taken when expressing personal views that these cannot be misinterpreted as belonging to Trust or LA, as the email address will part contain the Trust or LA name.
• If an urgent email is sent, you may want to follow this with a phone call.
• Never send emails that are offensive, threatening, defamatory or illegal. Emails have been used successfully as evidence in libel cases.
• Emails can be requested as part of the GDPR process – As they can be contractually binding, they should be factual. If it is an opinion, then it should be phrased as this in the email.

Security
• Staff are responsible for the security of their computer, and for protecting any information or data used and/or stored on it.
• Do not to leave a mailbox open and unattended, always keep it password protected. The account holder/s needs to strive to keep their passwords confidential; to prevent other users from accessing and sending emails from their account. Users may need to make their passwords known in the event of absence.
• Staff should be responsible for changing passwords on an agreed schedule to maintain security.
• Emails will only be monitored by the Head teacher in very exceptional circumstances.
• Longer term absent staff are aware that their email account may be opened by another member of senior staff. This will only be done with the head teachers authorisation.

Education

Pupils

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-school council, 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 (e.g. spotting and being discerning about 'fake news', part of the Year 5/6 PSHE programme of study).
[Update 2025]: In line with KCSIE 2025, children will also be taught about misinformation, disinformation, and conspiracy theories as online safety risks.

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 information as part of their induction programme, ensuring that they fully understand the school e-Safety Policy and Acceptable Use Policy.
f). Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate.
g). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety.
h). The school takes every opportunity to research and understand good practice that is taking place in other schools.

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/TrustEd executive team.
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

c). The school action plan indicates any planned action based on the above.

This policy is linked to the school's Safeguarding and Data Protection Policy.

Appendix 1: Acceptable User Policies

Parent/Carers Agreement

- I have read and discussed the Acceptable Use Policy with my child.
- I know that my child will receive digital (online) safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that the use of the internet using school equipment is monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task, particularly with new technologies and sudden online trends.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted. This includes concerns that inappropriate online material viewed at home is being discussed in school. I also understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school's behaviour and anti-bullying policy.
- I, together with my child, will support the school's approach to digital safety and will not deliberately upload or publish any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community, either on school or home devices. I will not name or identify members of staff on social media and any discussion of school will be professional and in line with the ethos of this policy.
- I will ensure that my child does not bring any device to school (including smartphones, smartwatches or cameras) that have the ability to photograph, video or audio record, unless by prior written agreement from Mr. O'Malley and Mr. Marsh. Any such agreement would be fully risk assessed.
- I know that I can speak to the school safeguarding team, my child's teacher or the Head Teacher if I have any concerns about digital safety.
- I will visit the school website http://www.alveleyprimary.co.uk/wellbeing-support/e-safety for more information about the school's approach to digital safety.
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety www.internetmatters.org, www.saferinternet.org.uk, and www.childnet.com for more information about keeping my child(ren) safe online.
- I will support the school and my child by sharing responsibility and role modelling safe and positive online behaviour for my child and by discussing online safety with them when they access technology at home.
- When communicating with school electronically, either via email or through learning portals such as Tapestry, all communication will be polite, professional and with a view to building a supportive collaboration for the benefit of pupils.

Key Stage 1
Pupil Agreement

- I will look after all the school IT equipment and use it properly.
- I will only share my username or password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I will only take a photograph or video of someone if they say it is alright.
- All of the messages I send will be polite.
- I will not post anything online which upsets other people.
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet.
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name.....

I confirm that I have read this policy with my child and have understood this policy.

Signed.....

Relationship to child……..

Key Stage 2
Pupil Agreement

- I will take care when using the school IT equipment and use it responsibly.
- I will keep my passwords private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images or messages.
- I will not interfere with anyone else's passwords, settings or files on the computer.
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I know that if I want to take a photograph or video of somebody, I will need their permission and my teacher's permission.
- I will not bring any device into school that can take photos, videos or audio recordings unless Mr. O'Malley and Mr. Marsh have given written agreement.
- Any messages I post online or send in an email will be polite and responsible. I will always ask myself "how would I feel if my parents or the other person's parents saw it?"
- I will not send or forward messages or create material which is deliberately intended to upset, embarrass or scare other people.
- I know I must take care about giving away my personal information and making contact with people I do not know when using the internet.
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I recognise that if online activities at home make me angry, cross or upset when I get into school and affect my work or playtimes, my teacher might need to speak to my parents/ carers.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may happen even if the activity was done outside school.

Pupil name.....

I confirm that I have read this policy with my child and have understood this policy.

Signed.....

Relationship to child……..

Staff Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 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 (e.g. 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 social networking sites in school in accordance with the school's policies.
- I will only communicate with learners 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 has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices 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 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's ICT systems without first discussing it with a member of SLT.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will 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, terrorist or extremist 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.
- 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 Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner 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 online systems 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).

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

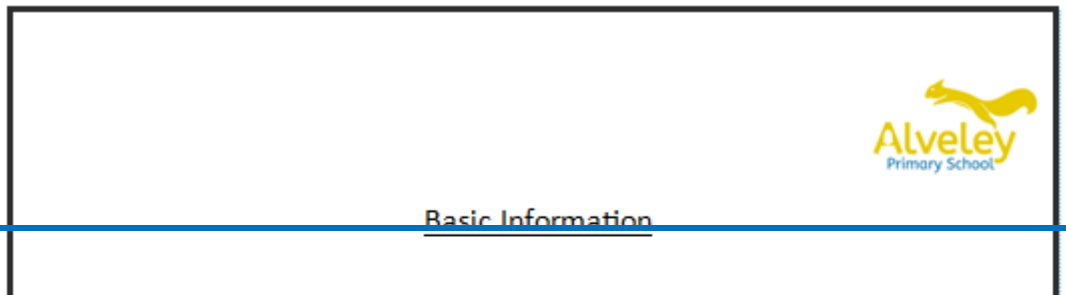
- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

Name.....

I confirm that I have read and understand this policy.

Signed.....

Appendix 2: General consent form



Alveley Primary School

Basic Information

Name :

Alveley Primary School

General Consent