Alveley Primary School
Member of the Bridgnorth Area Schools' Trust

ICT & E-Safety Policy 2018

This Policy links to the schools Data Protection Policy.

Contents Page

Responsibilities

The member of SLT responsible for e-safety is	Paul O’Malley
The Governor responsible for e-safety is	Geoff Baker
The e-Safety Co-ordinator is	Paul O’Malley

The e-Safety Co-ordinator is responsible for leading the e-Safety Committee, 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.

e-Safety Co-ordinator

The school e-Safety Co-ordinator is responsible for e-safety. He will meet with representatives from the following groups: SLT, Governors and teaching staff to discuss issues surrounding e-safety. Any issues will be fed back to the Governors.

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.

You 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.**

A copy of the pupil AUP will be signed as part of the school registration form. This 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 IT 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 monitored, 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. 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).**

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.

Visitors to school should ensure that mobile phones are switched off and handed in to the office.

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. Do not divulge your password to any person, or use another person's password. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle or drawer to which only you have access. 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, PED's 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 the event 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 teacher immediately – it is their responsibility to decide on appropriate action not the class teacher's.

Incidents which are not child protection issues but may require SLT/HOY intervention (eg cyberbullying) should be reported to the Head teacher asap.

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 should also be regularly reviewed to provide information to parents regarding e-safety.

Infringements and sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head teacher. Any student 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 Local Authority 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. Each year group's Class Teacher will indicate these opportunities within the provided planning.

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.

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 head teacher 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 BAST 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 the T drive 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-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 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/BAST executive Headteacher.
- 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 Data Protection Policy.

Appendices

Appendix 1 – Acceptable Use Policies (AUPs)

Alveley Primary School
ICT and E-safety, July 2018
Acceptable use policy for Pupils

Name: ………

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will: -

- keep my password a secret
- tell a member of staff if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell a member of staff if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable
- not give my mobile number, home number or address to anyone who is not a real friend
- only email people I know or if a member of staff agrees
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer
- never agree to meet a stranger.

Signed …………………………………………………. Date……………………………………

AUP for any adult working with learners

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. (Always check consent on SIMS)
- 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.
- Only use encrypted USB or hard drives if downloading pupil data.

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.

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 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, personal electronic 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

School Governors are also required to sign AUP for IT users as all school / BAST correspondence through the provided email address.

Appendix 2 – Data Consent Form GDPR Compliant

SCHOOL REGISTRATION FORM

Child's Name: ……………………………………….………

CONFIDENTIAL PERSONAL DETAILS FOR YOUR CHILD

ON COMPLETION, PLEASE RETURN TO THE ADMINISTRATOR AT ALVELEY PRIMARY SCHOOL

Birth Certificate:

Please could you provide school with a copy of your child's birth certificate (or a copy of your adoption certificate details where the original birth certificate is no longer relevant). This is simply to ensure that the correct legal name is on the school's database. If you wish, we can take a copy of your original certificate, just ask at reception. This is a request not a legal obligation. If you want your child to be "known as" another name please fill in tab 3. However, please note that the "known as" name cannot be used on certain aspects of our school system or on legal documents such as exam certificates. Once we have verified names any copies of documents will be destroyed in a safe manner.

Adopted from Care:

We have been informed by County that children adopted from care on or after **30 December 2005**, as well as those who left care under a special guardianship order or residence order (now known as a child arrangements order) attract a significant sum of additional funding to schools to be used to help support your child's academic progress and attainment.

If this is applicable to your child, we would be grateful if you could indicate (*with a tick*) which category below he/she falls into. It should be emphasised that the offering of this information is purely voluntary and parents are under no obligation to do so. If ticked we would ask for supporting paperwork, by way of a photocopy of the adoption order. Please feel free to block out any sensitive information e.g birth parents if you do not wish this to be revealed to the school.

Many thanks for your assistance with this information. Should this apply to you we would be grateful if you could tick below and return any supporting paperwork along with this registration form.
……….
I confirm that my child has been adopted and I have ticked the relevant box and provided a copy of the adoption order.

	Ceased to be looked after through adoption
	Ceased to be looked after through a Special Guardianship Order (SGO)
	Ceased to be looked after through a Residence Order (RO)
	Ceased to be looked after through a Child Arrangement Order (CAO)

For Office Use Only:

Date Received:	
Date entered on SIMS	
Birth Certificate	
LAC	
FSM	
Admission No:	

Please print all details clearly

1.	Your child’s Legal Surname	
2.	Your child’s Legal Forename(s)	
3.	Your child’s “known as” Surname *only complete if this is different from 1 above.*	
4.	Your child’s preferred forename	
5.	Your child’s date of birth (DDMMYYY)	
6.	Your child’s gender	Male □ Female □
7.	Your child’s full address	…………………………………………………………………… …………………………………………………………………… …………………………………………………………………… ……………………………………………………………………
8.	Postcode (**please print**) NB: this must match that on the Post Office website as the correct postcode is important. Insert a space where necessary (e.g. SY22 5JH)	

For most pupils your contacts will be placed automatically as Mother Priority 1, Father Priority 2, to enable our message alert system. Please mark clearly if you wish to change these priorities.

	CHILD’S PARENT/CARER DETAILS - Priority 1 This should be the Parent/Carer with whom your child resides for the majority of the week. If parents are separated but both have contact please provide full details **Priority 1 contact will be used for message alerts.**	
9.	Relationship to child	
10.	Title & Surname	
11.	First name	
12.	Full address (*if different from No. 7)*	…………………………………………………………………… …………………………………………………………………… …………………………………………………………………… ……………………………………………………………………
13.	Postcode (*see note in 8 above*)	
14.	Mobile telephone number Mobile numbers will be used for text messaging	
15.	Work telephone number	

16.	Home phone number	
17.	Email address (we will not divulge to any third party). Please print this in capital letters	Home:………………………………………………………. Work: ………………………………………………………
	CHILD'S PARENT/CARER DETAILS – Priority 2	
18.	Relationship to child	
19.	Title & Surname	
20.	First name	
21.	Full address (*if different from No. 7*)	……………………………………………………… ……………………………………………………… ……………………………………………………… ………………………………………………………
23.	Postcode (see note in 8 above)	□ □ □ □ □ □ □ □
24.	Mobile telephone number	
25.	Work telephone number	
26.	Home phone number	
27.	Email address	Home:………………………………………………………. Work: ………………………………………………………
28.	Are either Parent/Carer a member of the armed forces? Please circle Yes or No. (Your classification will be either PStat Cat 1 or 2; please note this only refers to regular forces and not the territorial's.)	Carer 1: Yes No Carer 2: Yes No
	In case we cannot reach either Parent/Guardian please provide an emergency contact who can act for you	
	Priority 3 - emergency contact	
29.	Relationship to child	
30.	First name	
31.	Title & Surname	
32.	Full address	………………………………………………………

		……………………………………………………… ………………………………………………………
33.	Postcode (see note in 8 above)	□□□□□□□□
34.	Home telephone number	
35.	Work telephone number	
36.	Mobile phone number	
	Priority 4 - emergency contact	
37.	Relationship to child	
38.	First name	
39.	Title & Surname	
40.	Full address	……………………………………………………… ……………………………………………………… ………………………………………………………
41.	Postcode (see note in 8 above)	□□□□□□□□
42.	Home telephone number	
43.	Work telephone number	
44.	Mobile phone number	
45.	Is your child currently in receipt of Free School Meals *(please tick)* *If you are out of area and receive FSM you will need to make an application to Shropshire County – please ask for an application form*	**Yes** □ **No** □
46.	Does your child have any **medical condition** (including asthma* or allergies) that we need to be aware of? If so, please provide full details including any medication that is being taken orally or by injection.	……………………………………………………… ……………………………………………………… ……………………………………………………… ……………………………………………………… ……………………………………………………… * If your child has asthma please tick on page 7 for use of an emergency inhaler if personal inhaler has been forgotten

47.	Please give the name of your child's **Medical Practice** *not the doctor's name* and contact telephone number.	**Practice** Name: …………………………………………… Phone No: ……………………………………………
48.	**Emergency medical aid** **(if you circle no, please let the school have details as to what you would not allow under this consent).**	Yes □ No □ …………………………………………………………………………… …………………………………………………………………………… …………………………………………………………………………… …………………………………………………………………………… …………………………………………………………………………… ……………………………………………………………………………

Ethnic/Cultural

On the next couple of pages we ask you about your child’s Ethnicity, Religion, Mother Tongue and language and how your child normally travels to school. You have every right to refuse to give any of the following information. However, if you complete each section, it may result in additional resources for the authority and the school. In relation to the mode of travel please be honest about this and where, for example, part of the journey is by car and part, say, is walking, please list the mode of transport used for the majority of the journey to school. This information can be used to great advantage for us when working on School Travel Plan and with Shirehall colleagues in obtaining funding for Safer Routes to School.

(A) Ethnicity (based on the Census ethnic categories)

Our ethnic background describes how we think of ourselves. This may be based on many things, including, for example, our skin colour, language, culture, ancestry or family history. ***Ethnic background is not the same as nationality or country of birth.*** Please study the list below and tick one box only to indicate the ethnic background of your child.

White		**School use (SIMS codes)**
♦ English	□	**WENG**
♦ Scottish	□	**WSCO**
♦ Welsh	□	**WWEL**
♦ Cornish	□	**WCOR**
♦ White Eastern European*	□	**WEEU**
♦ White Western European**	□	**WWEU**
♦ Other White British	□	**WOWB**
♦ Irish	□	**WIRI**
♦ Traveller of Irish Heritage	□	**WIRT**
♦ Gypsy/Roma	□	**WROM**
♦ Any other White background	□	**WOTW**
Mixed		
♦ White and Black Caribbean	□	**MWBC**
♦ White and Black African	□	**MWBA**
♦ White and Asian	□	**MWAS**
♦ Any other mixed background	□	**MOTH**
Asian or Asian British		
♦ Indian	□	**AIND**
♦ Pakistani	□	**APKN**
♦ Bangladeshi	□	**ABAN**
♦ Any other Asian background	□	**AOTH**
Black or Black British		
♦ Caribbean	□	**BCRB**
♦ African	□	**BAFR**
♦ Any other Black background	□	**BOTH**
Chinese	□	**CHNE**

Any other ethnic background	□	**OOTH**
I DO NOT wish to give this information	□	**REFU**

***** White Eastern European includes those from Belarus, Bosnia & Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Macedonia, Moldova, Poland, Romania, Russia, Serbia & Montenegro, Slovak, Slovenia and Ukraine. ** White Western European includes those from Austria, Belgium, Denmark, Finland, France, Germany, Holland, Italy, Luxembourg, Malta, Norway, Portugal, Spain, Sweden and Switzerland. **Please do not use WOTW if you can tick WEEU or WWEU**.

(B) <u>First Language</u>

"Mother tongue" or first language is the language to which your child was initially exposed during early development and continues to use this language in the home or the community. If a child acquired English, subsequent to early development, English cannot be denoted as their mother tongue no matter how proficient they have become. On this basis, please would you tick the appropriate box for what you therefore consider to be your child's mother tongue:

1. English □

2. Other than English □

(2a) *If you ticked 2 above, please would you tell us the most appropriate language you regard as your child's first language? (If we are unable to find this on our extensive listing of languages we may contact you for further clarification).*

....

(2b) Also could you then tick your child's Proficiency in English:-

a) New to English □ b) Early acquisition □ c) Developing confidence □

d) Competent □ e) Fluent □ f) Not yet assessed
□

3. I DO NOT wish to give this information □

(C) Home Language

Please state your child's home language, which is presently used in the home or in the community:

..
..

(D) **National Identity – Please tick your child's National Identity below:-**

English □ Welsh □ Scottish □ Irish □ British □ Other □

I do not wish to supply this information □

(E) Your Child's Country of Birth (*e.g. United Kingdom*):- …………………………………………..……

(F) Nationality (*e.g. United Kingdom*):- ……………………..............................……………….

(G) **Please would you let us have your family's religion by ticking one box below?**

1. Christian □ 2. Hindu □ 3. Jewish □ 4. Muslim □
5. Sikh □ 6. Buddhist □ 7. No Religion □ 8. Other Religion □
9. **I DO NOT** wish to give this information □

Mode of travel to school

Please tick the predominant mode of travel for your child – please tick ONE box only:

1. Bus – type not known *(see 5 or 6 as alternatives)*	□	**BNK**	6. Public Service Bus *	□	**PSB**
2. Car or Van	□	**CAR**	7. Taxi	□	**TXI**
3. Car Share *(with child/children from a different dwelling)*	□	**CRS**	8. Train	□	**TRN**
4. Cycle	□	**CYC**	9. Walk	□	**WLK**
5. Dedicated School Bus *	□	**DSB**	10. Other Please specify……………….……………	□	**OTH**

** Note – a public service vehicle will always have a service number, a dedicated school bus will not. If you are involved in a park and stride service this needs to be ticked as Car and not Walk. Mode of travel information is vital for School Travel Plans and will be updated in your child's class every January by the teacher checking that there has been no change in the way in which your son or daughter gets to our school.*

WE NEED YOUR PERMISSION FOR CERTAIN ASPECTS OF YOUR CHILD'S EDUCATION

Please would you tick **Yes** or **No** as appropriate. Thank you.

Permission to use an emergency inhaler *Only if your child has been **diagnosed with Asthma***	Yes □ No □
Accessing the internet at school	Yes □ No □
Photograph and name in our school prospectus	Yes □ No □
Photograph and name on our school website	Yes □ No □
Photograph and name in our school newsletter	Yes □ No □
Photograph and name in the local press *(to include sporting events)*	Yes □ No □
Video Imaging (*i.e. school productions)*	Yes □ No □
School Photographs	Yes □ No □
Copyright permission of any work produced *e.g for displays, competitions, articles etc*	Yes □ No □
Sex education	Yes □ No □

PLEASE SIGN BELOW AND RETURN COMPLETED FORM TO :-

Mrs S Green
Alveley Primary School
Daddlebrook Road
Alveley
WV15 6JT

I acknowledge that the details and information I have provided must only be used for the purposes indicated by the paragraph on page 1.

Signed: ……………………………………………………….

Date: ……………………………………………………….

This document can be made available in other formats, e.g. Braille, as well as other languages. Please tell us if that is the case and we will make arrangements with Shirehall to ensure that you receive one as soon as possible. Please note that documents requested in other languages can take between four and six weeks to supply.

APPENDIX 3 – Staff Summary sheet IT Update linked to GDPR

Alveley Primary School – ICT & GDPR Summary Guide for staff.

The full ICT & E-Safety policy can be found on the school's website.

Do

- Always inform the E-Safety co-ordinator (POM) of any issues. These will be recorded and reviewed to ensure further improvements.
- Always review and update your password termly. These should be strong (8 characters and contain numbers and letters)
- Ensure that your allocated school device (laptop/i-pad) is only used by yourself and only for school related business.
- If your mobile phone or personal computer is linked to your Office 365 account you must ensure that you are the only person who has access to this. Check that you have logged out correctly and that you have not downloaded any sensitive data to your device. The device must be password protected.
- Check the register of consent in SIMS if you want to take/use a photo of a student.
- Please ask any visitors to school to ensure that mobile phones are switched off.
- Only use encrypted USB or encrypted hard drives to store personal data – best practice is to use the cloud (Office 365).
- If transporting ICT equipment off site this must be transported in your boot and not left in it overnight. It is your responsibility to ensure they are stored safely and securely at home.
- The school recommends that the use of social media accounts is limited to protect yourselves.
- If you have social media accounts check them to ensure privacy settings are robust.
- Protect yourself if you use social media by not accepting friend requests from parents, pupils (current or former). If you need to do this then please write to the Head Teacher outlining your reasons.
- Remember that sharing, forwarding posts or emails can be viewed as a sign of endorsement.
- Check any groups that you may join – if it is open does it contain pupils, parents?
- When sending email:
    - Check the correct recipients
    - Write it in a professional manner
    - Always write the email first and then add the address.
    - Take care if you 'reply all'
    - If you accidently send the email to the wrong address try to retrieve it. If this is not possible then you MUST inform the schools Data Protection Officer.
- When receiving emails:
    - Check the address and never open unfamiliar emails in the event of a virus or malware.
    - Check regularly and delete unwanted emails promptly. If files are important they should be saved to the cloud drive and not on the email system to reduce risk of a data breach.
- Remember that an email can be contractually binding- therefore take care if expressing your opinion.

- If you take pupil information home (planning folders, pupil files) you must do this in a secure manner. It should be transported in a separate bag in your boot. When at home these must not be left in the boot, but secured safely. Any files that are taken home must have a copy of the schools contact details if found.
- In school pupil information should be stored securely in lockable drawers, locked filing cabinets and offices.

If you feel that there has been a data breach you must inform the schools Data Protection Officer immediately – See data breach flow chart.

Don’t

- Leave your laptop unlocked in school (Control – Alt – Delete to lock) this has the potential to be a data breach if pupils can access emails or Sims. These should never be broadcast through a projector.
- Divulge your password to anyone else. These must be changed immediately if you feel that your account has been compromised.
- Install software onto your device without contacting the ICT Network Manager.
- Purchase software that requires personal data of students without checking with the Data Protection Officer to ensure GDPR compliance. If it is not compliant it will not be installed.
- Use your own personal devices to take pictures of pupils or to phone text parents – if you need to these must be removed as soon as possible and stored on the school’s cloud system.
- Share personal contact details with parents such as personal emails or phone numbers.
- Use social media to discuss school related business at all that may be construed as defamatory or discriminatory.
- Register any social media accounts to your school account
- Send sensitive data via email to an unknown contact – Best practice would be to use encrypted email or to pass word protect a document and then phone the recipient with the password.
- Accept friend requests from parents, pupils or past pupils. Block any requests of this type.
- Give personal information to a third party without checking (even from the police)
- Leave sensitive data in staff pigeon holes – always pass face to face.

Remember these guidelines are set to protect all users from any breaches or misuse of ICT equipment, and systems.