Send C of E Primary School

E-Safety Policy

Originally approved	November 2021
Date for revision	November 2023
Policy Originator	Melissa Perkins
Reviewed by	Learning and Achievement Committee

Childhood matters to us: it is short, precious and cannot be repeated. Our Christian values are rooted in God. Growing in love, every child reaches their spiritual and academic potential. Our learners use their resilience, curiosity and independence to become fruitful and effective global citizens.

With the Holy Spirit by our side, we can achieve anything!

Technology has revolutionised the movement, access and storage of information for all schools. More powerful computers, media, Internet, and digital recorders give increased opportunities to collaborate and communicate, changing when and where learning takes place. What we must ensure is that children are able to utilise these resources in a safe and considered way.

Aims:

Our school recognises that learning is a lifelong process and that e-learning is an integral part of education. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe and how to take responsibility for others' safety.

The school is committed to the continuing development of our technology infrastructure and the embracing of new technologies to maximise the opportunities and communication for all pupils, staff, parents and the wider community.

The e-safety policy covers the use of all technology that can access the school network and Internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, staff and children's iPad's mobile phones, tablets and hand held games consoles used on the school site.

However, no technology is without risk and keeping pupils safe is of paramount importance. Therefore, this policy aims to identify the risks and explain procedures for ensuring that e-learning is as safe as we can make it. **This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.**

This policy should be read in conjunction with the school's Teaching and Learning Policy and Health and Safety Policy.

1. **Safety**

i. **Safeguarding**:

- The school is proactive in dealing with child protection issues on an individual basis and issues will be recorded on the school's Child Protection Report Form and the CPOMS system if required.
- Where appropriate, our ICT engineers will be informed of the necessary actions to be put into place.
- Each child is taught to understand and abide to acceptable online usage through our child friendly e-safety agreement (see appendix 1), which are posted in every classroom.
- Each child is taught to follow the SMART rules of Internet usage (see appendix 2) to ensure they are working responsibly online and understands what actions to take if they feel uncomfortable, threatened or bullied.
- iPads are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website, Twitter or the newsletter. On the website, we never state a child's full name with their image. This is in line with guidance as set out in Surrey Safeguarding Children Board Guidance on using images of children. https://www.surreycc.gov.uk/__data/assets/pdf_file/0008/11312/SSCB-Guidance-using-images-of-children.pdf. The school will happily remove any image of a child on the school website at their parent's request.
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying as part of the PSHCE/RSE curriculum.

ii. School equipment:

- All electrical equipment in the school is tested annually to ensure that it is safe to use. Pupils are taught about the dangers of electricity as part of the science and PSHCE curriculum.
- Computers and iPads should be cleaned and sanitised regularly.
- Pupils are taught the correct way to use technology.

iii. School Network:

- All child iPads will have a generic unlock code children will therefore be able to access these independently. There will be strict filtering in place to ensure that they are accessing appropriate materials on the school network/WiFi.
- Pupils are taught how to save their work into their year group area on Google Drive.
- Pupils are taught not to access another user's work without permission.
- Pupils are taught to only print when necessary to save resources for financial and environmental reasons.
- Only the network administrators are permitted to install software on to iPads. Pupils are taught that the network or an application may not function properly if apps are installed.
- The network administrators can monitor all users of the network remotely. Pupils are taught that their use of the network can be monitored.

- Staff are able to log into the school network remotely at home. They must ensure that they follow the appropriate GDPR compliant login systems. When working remotely, staff must log in and out of the systems and ensure no-one else has access to them.

iv. Internet usage:

Use of websites and online tools:-

- When using an Internet enabled computer or device (iPads/laptop/computer), all access to the Internet is filtered by our Internet Service Provider to a standard agreed by Surrey, alongside other filter lists. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses, which are considered to be unacceptable. However, no system is 100% safe and we teach pupils how to assess and manage risk, to gain knowledge and understanding to keep themselves safe when using the Internet. We also work to bridge the gap between the school IT systems and the more open systems outside school. Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, and not child-friendly or can damage your computer.
- For online tools pupils are allocated a unique username and password. *Pupils are taught to keep their passwords safe and that they should only access systems using their username or the group username.*
- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents.
- The school will ensure that its networks have virus and anti-spam protection.
- The school website may contain samples of pupils work as well as school policies, newsletters and other information. We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.
- Systems will be in place to ensure that Internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the Internet via school equipment for anyone not employed by the school, is filtered and monitored.

Use of emailing**:**

- Some pupils will have their own web based e-mail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for e-mail usage. Therefore we regret that we do not permit the use of personalised e-mail accounts by pupils at school or at home for school purposes. *Pupils are taught that using a personalised e-mail account in school or for school use is not permitted.*
- Pupils are permitted to use their class email account to access their class projects and email work to their teacher for review or printing. Class teachers are expected to change their class password each year to ensure other classes cannot access other class folders. Pupils are taught of the importance of respecting other children's work and keeping passwords safe from others.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Complaints of Internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school's child protection procedures.

2. Other Devices

v. Mobile Phones:

- Pupils are not permitted to have mobile phones upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However we discourage this on security grounds as they are easily lost, damaged or stolen. (Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day.)
- Staff members are not permitted to use mobile phones in working time for calls, text, e-mail, social media or photography. Please refer to the 'use of mobile phone' policy.

vi. Podcasting**:**

- Pupils will be given opportunities to create oral recordings. Some of these recordings may be made available as podcasts through the Internet so that shared with interested members of the school community.

3. Copyright

- Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws and staff should be mindful not to infringe on copyright laws. However, some can be used for educational reasons, without permission, provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology.
- As the school holds collective worship copyright licences we have to report the songs we sing in our assemblies. This helps to ensure royalties are fairly paid to rights holders. This is through the Collective Worship Music Reproduction Licence (CWMRL) under Christian Copyright Licensing International Ltd (CCLI)
- It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information.

4. Parental Education

- Send CofE offers regular informative sessions for parents annually and in response to the current demand.
- The use of newsletters, Twitter and the website are used proactively to inform parents of updates and e-safety information.

5. Acceptable Use

The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

- School systems should only be used for legitimate school business relating to the administration of the school or Teaching and Learning.
- All communication between staff and pupils or families will take place using school equipment and/or school accounts.
- Staff should comply the Staff Code of Conduct at all times including when using any IT equipment (please refer to Staff Code of Conduct).

- Social networking sites, media sharing and micro blog web sites (such as Facebook, YouTube, Instagram, Twitter, TikTok and Pinterest) should not be used on the school network with the exception of videos used as a teaching tool. Pupils are taught about acceptable use of these sites. We expect pupils and staff not to access these sites in school.
- Outside school we expect pupils and members of staff not to post anything that might bring the school into disrepute. Online activity in and out of school should take into account the feelings of others and is appropriate for their situation as a member of the school community. Staff are not permitted to post pictures from school life on public sites and should be very careful about posting any personal information that could be linked to them in their school role e.g. house numbers in photos. Staff users of social media sites should review their privacy settings.
- The school will monitor public statements made about our school and apply to remove any content we consider harmful or derogatory.
- The school Twitter account is operated by a designated member of SLT and the Office Team and is used to promote the school's activities locally.
- Personal devices may not be used for school purposes and may not be connected to the school network. As a school we cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Acceptable use posters are displayed in the staff room and on iPad charging trollies.

6. Appendix 1:

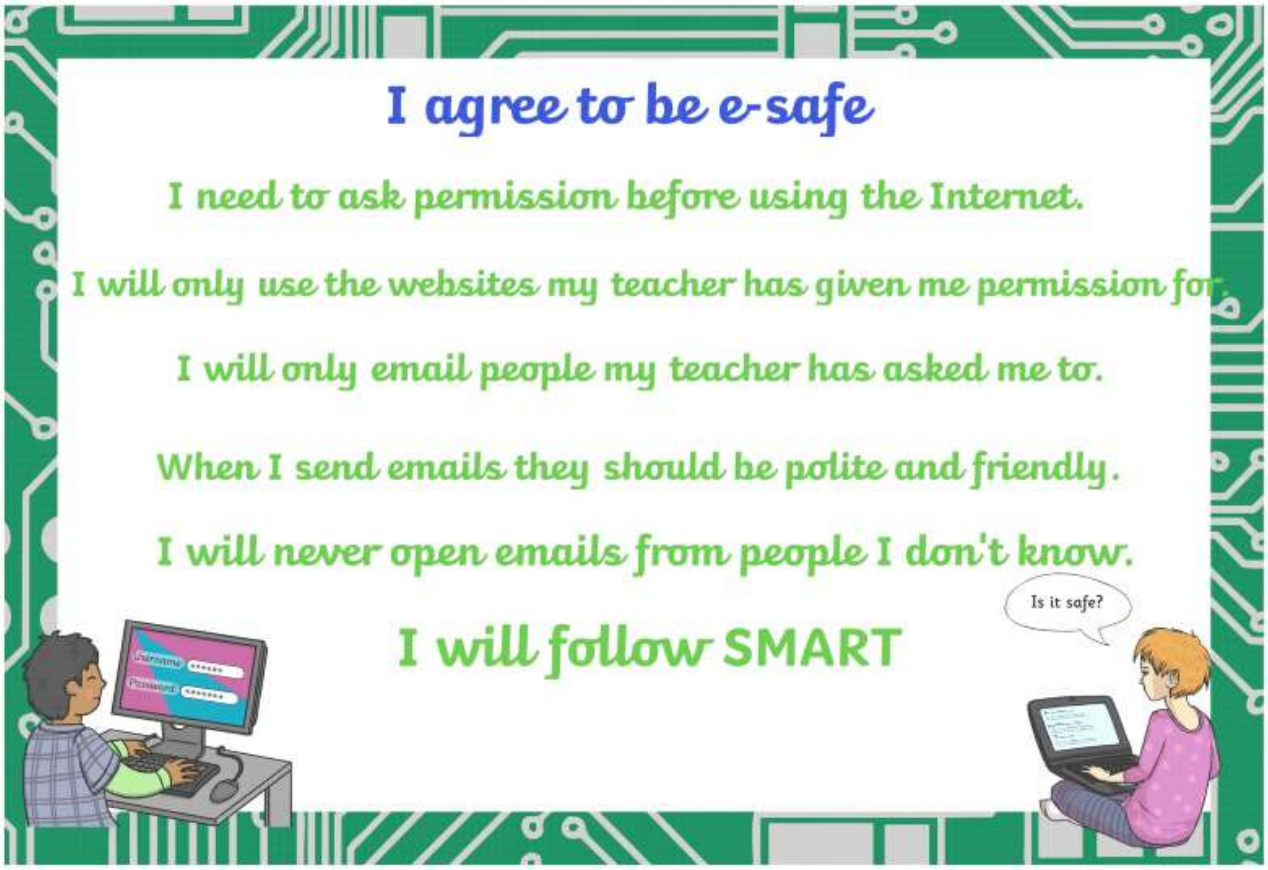
vii. Authorising Access:

- All staff must read and sign the Staff 'Acceptable Use Policy' before accessing the school IT systems Appendix 1.
- Parents will be asked to understand and read how the school uses technology for teaching and learning and contact the school with any concerns or questions by their child as part of the school's Home School Agreement.
- All children need to agree and comply with the pupil 'Agreeable Use Policy' in order to gain access to the school IT systems and to the internet. Appendix 4.
- Children will be reminded about the contents of the 'Agreeable Use Policy' as part of their e-safety education.

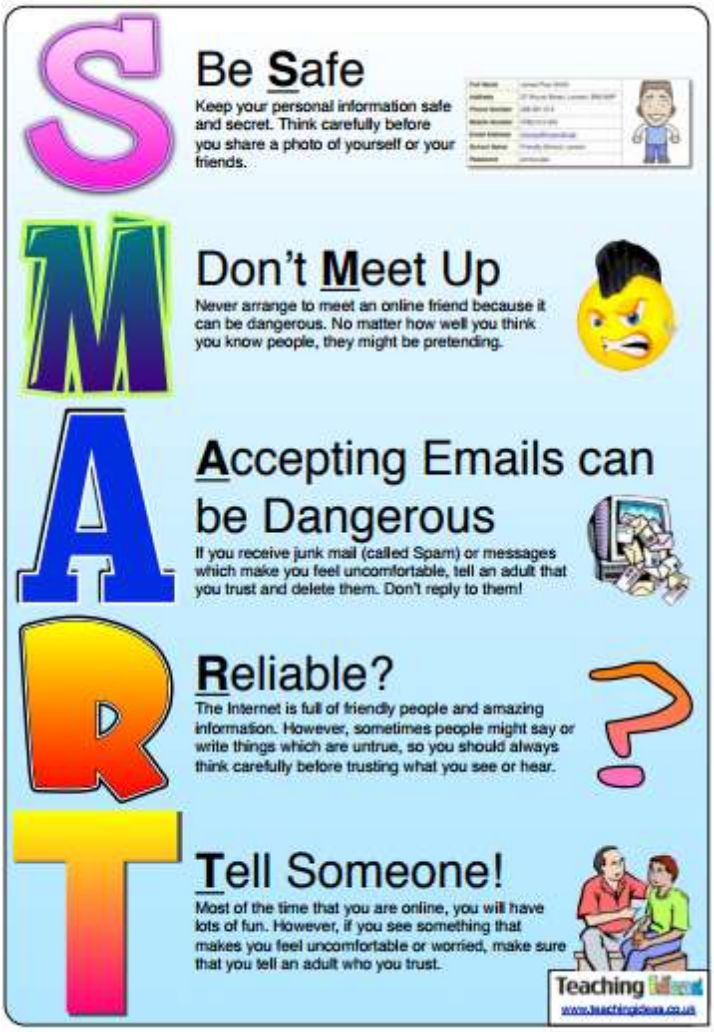
viii. Data Protection Act:

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs - http://www.justice.gov.uk/
- The school Data Protection Policy must be referred to in compliance with this area.

7. Appendix 2: Acceptable Use Poster



Appendix 3: SMART poster



8. Appendix 3: Staff 'Acceptable Use Policy'

Send Church of England Primary School has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held and complies with the requirements of the Data Protection Act 1998.

The use of portable computer devices increases the risks associated with the secure storage of data. The purpose of this policy is to set out the criteria for the conditions relating to the use of school owned or personal removable media (e.g. flash drives/ memory sticks, external hard drives).

Staff using such devices will be asked annually to sign to say that they have read and understood the information in this policy.

For the purpose of this policy, the term "laptop" is used to describe any portable computer device including laptops, notebooks, tablet PCs, cameras, flash drives on which school data may be stored. Your laptop is a valuable asset and an essential business tool. It needs to be protected, as does the information it stores. Remember that the laptop and the information that it contains could be valuable to thieves. By following the simple security measures listed below, you can help protect yourself and your laptop.

Staff Guidelines – General

Responsibilities

Computers, laptops, netbooks, iPads and other networked resources, including Internet access, are available to staff in the school. These resources are intended for educational purposes, and may only be used for legal activities consistent with the rules and policies of the school.

It is expected that staff will use ICT resources as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the use of the online curriculum. The ICT resources are provided and maintained for the benefit of all staff, who are encouraged to use the online resources available to them.

Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn. Teachers/ members of staff must take personal responsibility for the security of the equipment, software and data in their care and abide by the following:

Computers, Laptops and other electronics at home or school

- Laptops in cars must be stored out of sight (e.g. in covered boot). Laptops should never be left in a vehicle for prolonged periods of time or overnight.
- Always leave your laptop in a safe, out of sight location when it is not in use in school.
- Ensure your laptop is not used by unauthorised persons. This includes family and friends as there is a risk that school information could be compromised.
- Take reasonable steps to ensure that the laptop is not damaged through misuse.
- When travelling, laptops should not be left unattended in public places.
- Remain particularly vigilant when using your laptop and try to refrain from using it in public places e.g. library, railway station.
- Return the laptop to school for regular health checks or when requested and ensure that the laptop antivirus software is updated.
- Return the laptop before leaving the employment of the school
- Do not install, attempt to install, or store programs of any type that are not from a reputable source and a requirement of the establishment.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.

- Do not use the computers for commercial purposes, e.g. buying or selling goods unless they are for a specific educational need.
- Do not open files brought in on removable media (such as CDs, flash drives, etc.) until they have been checked with antivirus software and been found to be clean of viruses.
- Do not connect any mobile equipment to the network until they have been checked with antivirus software and been found to be clean of viruses.

Security & Privacy

Networked storage areas and other external storage hardware (USB's and hardrives etc) are the responsibility of the school. Files and communications may be reviewed to ensure that users are using the system responsibly.

- Passwords should be kept safe. Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet personal information, your home address, your telephone number or your school's name, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Do not intentionally allow unauthorised access to data and resources on the school network system or other systems.
- Do not intentionally use the computers to cause corruption or destruction of other users' data, or violate the privacy of other users.
- Report any possible security breaches to the Headteacher or School Business Manager immediately.
- Ensure that the school office has noted any serial numbers for the equipment register and that asset tags have been created and attached where necessary.
- Back up your files regularly and store them securely.
  If you are attacked/ mugged for your laptop, hand it over. It can be replaced but you cannot!

Internet (please also refer to the school e-Safety policy)

- Do not access the Internet unless for school related activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials, which are unlawful, obscene or abusive.
- Abide by copyright laws by respecting the work and ownership rights of people outside the school, as well as other students or staff.
- Do not engage in 'chat' activities of a personal nature over the Internet including social networking sites, blogs and forums during school time.
- Do not post any e-comments that represent the school unless authorised by the Senior Leadership Team (SLT).

Email

- Your school e-mail account will be your principal point of contact for all electronic communication with the school.
- Never use strong language, swearing or aggressive behaviour.

- Never open attachments to emails unless they come from someone you know and trust. (They could contain viruses or other programs that can destroy all the information and software on your computer).
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content (All such messages must be reported immediately to a member of the SLT)

Specifically for laptops for teachers

- Do not install, attempt to install, device drivers and software on the laptops without permission from the network administrator.
- No settings must be changed on your laptop unless authorised by the ICT department this includes Internet settings, browsers and system preferences
- You are continuously responsible for the laptop issued. Any damage must be reported to Mrs Weedon, SBM immediately.
- You are responsible for the repair and maintenance costs of laptops (hardware and software) necessary due to negligence or misuse.
- You must not allow any external agency or support service to tamper with school laptops hardware or software.
- Appropriate and safe care and storage of school laptops is expected at home.
- Do not access any other non-internet network from your laptop.
- Laptops must be connected to the network at least once per week to allow updates to occur.

Services

Send C of E Primary School will endeavour to alert staff of any network related issues that may affect the use of IT within the school network. There are no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any loss of data as a result of service interruptions from external systems and providers including the internet service providers, server malfunctions or delay and non-delivery of devices and or software.

The school will keep a list of serial numbers for laptop devices and will notify the police if a school owned device is stolen. The school will obtain a crime reference number and advise the school's insurers.

Use of any information obtained via the network is at your own risk.

Staff Agreement Form

Please read the ICT Acceptable Use Policy carefully.

I understand that the school uses a filtered internet service and takes every reasonable precaution to ensure that I cannot access inappropriate materials, and I acknowledge that I will be deemed responsible for my own action when selecting, sharing and exploring information and media.

If any teacher violates these provisions, access to a laptop, the school network and the Internet will be denied and the teacher may be subject to disciplinary action.

I have read and understand the above and agree to use the School ICT facilities at Send C of E Primary School.

Signed:

Date:

Equipment type:

Serial no:

9. Appendix 4: Tapestry Agreement

Dear Parents and Carers,

All early years children attending our school have a personal on-line Learning Journey which records photos, observations and comments, in line with the Early Years curriculum, to build up a record of your child's learning experiences during their time with us.

We use Tapestry, a system, which is hosted in the UK on secure servers. These servers conform to very high environmental standards and are proactively managed 24 hours a day. Each Tapestry account has its own database and the code itself is developed using hack-resistant techniques. Filenames are encoded for uploaded, videos and images, making Tapestry a safe and secure on-line Learning Journey tool. The benefits to yourselves from Tapestry being on-line means you will have secure access (via a website which you login to using your email address and a password) to your child's Learning Journey and, in addition to viewing our contributions, we encourage you to add to it by uploading photos and comments, or commenting on observations made by us.

Each class has their own secure Tapestry website, which once you have provided the school with an e-mail address we will be able to set you up with an account. We will also give you detailed information on how to view/use your child's Learning Journey. If you do not have access to e-mail your child is still able to have an online Learning Journey which you can access through the use of school computer, which can be organised with your child's class teacher. It is also possible to provide print outs of the Learning Journeys, each child will receive a full print out of their Learning Journey at the end of the Reception Year.

In order for your child's Learning Journey to be created, please give us permission by completing the attached slip. Also if you provide your E-mail address we will set up an account enabling you to access your child's learning journey via the secure Tapestry website for your child's class. (Please note, each parent only has access to their own child's Learning Journey).

If you have any questions or queries about the on-line Learning Journeys please do not hesitate to ask your child's class teacher.

Many Thanks

Mrs R Bruton
EYFS Leader

TAPESTRY
ONLINE LEARNING JOURNAL

10. Tapestry Permission Slip

1) I agree to my child having a Tapestry Online Learning Journey.

2) I agree not to post any content from my child's learning journey on any social networking site, e.g. Facebook.

3) I give permission for my child's image to appear in photographs/videos in other children's learning journey. (We try to avoid this but it is not always possible when children are playing closely together).

I give permission for Send C of E Primary to create an online Tapestry Learning Journey for:

(Name of child).

The e-mail address I would like to link with the account so I have access to my child's Learning Journey is:

(provide your e-mail address)

Parent/Carer signature: _____

OR

If you do not have access to e-mail please tick this box and you will be able to view your child's learning Journey using school equipment during specific times throughout the year.

☐