Policy: Remote Learning

Date: April 2021 (Pupil Acceptable Use Update)

See also Partial Closures Spring 2021 Addendum to This Policy – approved by Covid-19 Sub-Committee of the Governing Board 13/01/2021

Date created:	17th September, consultation with staff 17 – 21st September, amended 13th Jan 2021 and Feb 21 and additional addendum for Spring Term Partial Closures, April 21 pupil acceptable use update
Responsible:	Senior Leadership Team
Responsible Committee:	Covid-19 Committee
Date Ratified:	22nd September 2020 amendments approved by Covid-19 Sub-committee
Date to be reviewed:	Every 3 months during Covid-19 pandemic and annually thereafter

Contents

---

1. Aims

This remote learning policy aims to:

- Ensure consistency in the approach to remote learning for pupils who are self-isolating due to Covid-19 restrictions
- Set out expectations for all members of the school community with regards to remote learning
- Provide appropriate guidelines for data protection

2. Roles and responsibilities

2.1 Teachers

- All teachers must adhere to the Acceptable use agreement (Staff, Governors, Volunteers and Visitors) - Appendix 3
- When providing remote learning, teachers must be available between 9am to 4:00 pm Monday to Friday
- If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they must report this using the normal absence procedure.

When providing remote learning, teachers are responsible for:

- Providing learning for the pupils in their class via Google Classroom
- Delivering learning in liaison with Year Group colleagues

The **minimum requirements** for Google Classroom provision in the event of a **whole class/year group/school** closure are as follows:

- The class time table of subjects (not timings) will be followed
- A Daily English Live Lesson and a Daily Maths Video Lesson (White Rose Maths). Input of approximately 20 minutes followed by differentiated follow-up activities. The teacher and TA

should remain online in a live session for the duration of the allocated hour to allow targeted support where needed.

The input of the live lessons must be recorded and uploaded as soon as possible on the same day for pupils unable to attend the live screening. Recording must start after greetings and register at which point pupil cameras and microphones should be switched off. (Individual microphones can then be turned on when answering questions/contributing to the lesson). Recording must stop at the end of the input to allow parents and children to seek additional clarification in confidence.

- Maths and English lessons will be uploaded each day Mon-Friday during Covid-19 closures. Other learning activities can be either uploaded together at the start of the week or on a daily basis depending the circumstances of each individual teacher. All non-live learning must be uploaded by 9am of the day it appears on the class timetable.
- Teachers should provide a clear daily or weekly timetable via Google Classroom to support families in organising their time and resources
- Teachers should ensure that activities and support materials are uploaded in a clearly accessible, labelled way with written or recorded instruction
- Additional Live sessions and Videoed sessions will be provided where possible – eg French, story reading, collective worships, PE challenges and assemblies for example.

9am Live English lesson	Maths lesson video	Afternoon timetable – wider curriculum

- When setting work on Google Classroom, a deadline must be clearly provided.
- Feedback on submitted work should be given where possible if submitted by the given deadline. Recorded verbal feedback is a recommended approach in addition to other written forms of feedback
- Pupils can submit work after the deadline but there is no requirement for feedback in these cases
- Most set activities can be submitted online. All children will also be provided with a home-learning book to use when isolating due to Covid-19 restrictions. It should not be used for other purposes. Any work set via Google Classroom can also be recorded in this book, photographs of completed work can be submitted via Google Classroom.
- PPA cover staff should also provide learning via Google Classroom.
- Class teachers are responsible for the provision of all the English and Maths lessons.
- Class teachers must maintain a record of pupil engagement in remote learning and should contact parents where pupils are not accessing GC to provide support. The IT technician can support technical difficulties. Where there remain concerns, the class teacher must alert a member of SLT who will make contact with parents/carers/pupils.
- If the whole school is forced to close over an extended period of time, teachers will make direct contact with parents/carers/pupils
- Any member of staff delivering live or recorded lessons must adhere to the staff dress code
- When delivering live or recorded lessons, avoid areas with any background noise and ensure that nothing inappropriate is in the background.

It is understood that not all aspects of the planned wider curriculum can be delivered remotely, however, all curriculum subjects will be delivered wherever possible.

Where **individuals or small groups of pupils** are self-isolating due to Covid-19 restrictions, the following requirements are in place:

Weekly learning activities will be set via *Google Classroom Classwork*, within the 'Self-isolating Individuals' section. Weekly homework for all pupils will also be provided via Google Classroom. Remote learning will include access to live or recorded sessions. It is recognised that it will not be possible or suitable to share all learning materials, resources or strategies used within

classroom setting with self-isolating individuals via Google Classroom. Feedback will be given to submitted work **where possible** within the constraints of the teacher's working day.

2.2 Teaching assistants

- All Teaching Assistants must adhere to the Acceptable use agreement (Staff, Governors, Volunteers and Visitors) - Appendix 3
- In the event of closure of their allocated 'bubble', teaching assistants are required, under the direction of the class teacher, to assist with remote learning. Teaching assistants must be available during their normal working hours, following the subject daily timetable unless otherwise directed by the class teacher.
- If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure.
- Any member of staff delivering live or recorded lessons must adhere to the staff dress code
- When delivering live or recorded lessons, avoid areas with any background noise and ensure that nothing inappropriate is in the background.
- SEND 1:1 TAs should provide targeted activities and feedback for the pupil/s they support, under the direction of the class teacher or Inclusion Manager

2.3 Subject leaders

Alongside their teaching responsibilities, subject leaders with designated management time, are responsible for:

- Considering whether any aspects of the subject curriculum need to change to accommodate remote learning
- Working with teachers teaching their subject remotely to make sure all work set is appropriate and consistent
- Monitoring the remote work set on Google Classroom by teachers in their subject and providing nest-step developmental feedback where appropriate
- Alerting teachers to resources they can use to teach their subject remotely

2.4 Senior leaders (SLT)

Alongside any teaching responsibilities, senior leaders are responsible for:

- Co-ordinating the remote learning approach across the school
- Monitoring the effectiveness of remote learning – through regular meetings (remote) with teachers and subject leaders, reviewing work set or seeking feedback from pupils and parents
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations

The Inclusion Manager is also responsible for coordinating the remote learning provision for pupils with EHCPs and monitoring provision for other pupils with SEND

2.5 Designated safeguarding lead

The DSL is responsible for:

- Ensuring that the Child Protection Policy and Covid-19 addendum are adhered to
- Liaising with social workers and other external agencies involved with isolating families
- Liaising with families of identified vulnerable pupils during periods of isolation

2.6 IT technician

IT staff are responsible for:

- Fixing issues with systems used to set and collect work
- Helping staff and parents with any technical issues they're experiencing
- Reviewing the security of remote learning systems and flagging any data protection breaches to the data protection officer
- Assisting pupils and parents with accessing the internet or devices

2.7 Pupils and parents

Pupils

Staff can expect pupils - with the support of parents/carers - to:

- Complete work to the deadline set by teachers
- Wear suitable clothing
- Access the live lesson from a suitable location in the house e.g. not bedroom
- Submit completed work to Google Classroom where possible
- Use the Home Learning Book for work that cannot be completed online
- Attend live lessons or watch the recorded versions
- When joining live lessons, arrive on time and with their parent's agreement, ensure microphone and video are turned on for the initial greeting and registration. The teacher will then turn them off during the teaching input
- If wishing to answer or contribute during a live session, use the 'hands up' facility or the 'chat' if their microphone does not work. The teacher will know that the pupil wants to contribute. Please be patient, not every child can be chosen - just like in the normal classroom.
- If chosen to contribute an answer or comment, unmute their own microphone for the duration of the contribution
- Seek help if they need it, from teachers or teaching assistants - through the Google Meet live support session after the main live/video input or through the Google Classroom Stream. (parents can also contact the teacher directly be email)
- Alert teachers if they are not able to complete work - through the Google Classroom Stream. (parents can also contact the teacher directly by email)
- Adhere to the Acceptable Use Agreement (Pupils and Parents/Carers) (appendix 1 and also signed in pupil planners)
- Ensure that all comments within Google Classroom stream are related to the work - greetings are permitted but must be of a positive nature
- All language used within pupil comments and class stream must be appropriate and respectful
- All pupils must adhere to the school Behaviour Policy
- Pupils must recognise and respect that the materials provided via Google Classroom are for the exclusive use of St Bernadette's pupils and must not be shared without the consent of the author.

Parents/Carers

Staff can expect parents with children learning remotely to support their child with all of the above expectations and also:

- Make the school aware if their child is sick by following the usual absence procedures

- Report any positive cases of Covid-19 immediately to the school office or the designated Covid-19 phone line out of school hours - 07488343463
- Email the class teacher if, for whatever other reason, their child cannot complete the work set
- Email the class teacher directly, from parental email address, with any questions or queries relating to the set work
- Staff members can be contacted by email; use surname followed by first initial followed by @stbernadettesschool.com e.g. Jane Zamora's email address: ZamoraJ@stbernadettesschool.com See the website staff page for staff names: https://www.stbernadettesschool.com/staffing/
- Be aware that a number of our staff members work part time. No staff member is expected to check or answer work-related emails outside of their working hours, at weekends, or when off sick.
- To allow the live lessons to flow effectively, refrain from making contributions or comments during the live input unless invited to by the teacher.
- Ensure your child and anyone else in the household during a live lesson is wearing appropriate clothing
- Request any clarification or queries relating specifically to their child during a live session, only after the live input has concluded - the teacher will remain online within Google Meet to address these.
- Recognise and respect that the materials provided via Google Classroom are for the exclusive use of St Bernadette's pupils and must not be shared without the consent of the author.

2.8 Governing board

The governing board is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible - There is a cascade system in place during the pandemic whereby the Headteacher provides weekly progress and issues Briefings to the Covid-19 Sub Committee. The full board consequently receive weekly written Board Briefings from the Chair. All actions by the COVID-19 Sub Committee are then reported to the next Full Governing Board Meeting.
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

3. Who to contact for Staff

If **staff** have any questions or concerns about remote learning, they should contact the following individuals:

- Issues in setting work – liaise with year group teacher colleague, line manager or the relevant subject lead or Inclusion Manager
- Issues with behaviour – contact line manager or member of SLT and liaise directly with parent/carer
- Issues with IT – contact IT technician
- Issues with their own workload or wellbeing – contact the line manager or member of SLT
- Concerns about data protection – queries and concerns – contact the IT technician or SLT. If reporting a data breach contact the data protection officer
- Concerns about safeguarding – contact the DSL or deputy DSL

4. Data protection

4.1 Accessing personal data

When accessing personal data for remote learning purposes, all staff members will:

- Use their allocated staff laptop and the school's VPN

4.2 Processing personal data

Staff members may need to collect and/or share personal data such as email addresses as part of the remote learning system. As long as this processing is necessary for the school's official functions, individuals will not need to give permission for this to happen.

However, staff are reminded to collect and/or share as little personal data as possible online.

4.3 Keeping devices secure

In order to keep their allocated staff laptops secure, all staff must adhere to the Acceptable use agreement (Staff, Governors, Volunteers and Visitors) - Appendix 2 and signed annually.

5. Safeguarding

All staff must adhere to the Child Protection Policy and Covid-19 addendum at all times. These are available via the T-drive, the school website and the staffroom.

6. Monitoring arrangements

This policy will be reviewed every 3 months during the Covid-19 pandemic and annually thereafter. At every review, it will be approved by the Covid-19 Governing Committee.

7. Links with other policies

This policy is linked to our:

- Behaviour policy
- Child protection policy and coronavirus addendum to our child protection policy
- Data protection policy and privacy notices
- Home-school agreement
- ICT and internet Acceptable Use Agreements (see appendices 2 & 3)
- Online and Computer safety policy
- National School Closures Addendum to the Remote Learning Policy

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

Rules for Responsible Internet Use for Pupils

- @ I will not give out my own details such as my name, phone number, school name or home address, unless my teacher/parents/carer gives me permission.
- @ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- @ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- @ I will not send photographs or videos or any other information about myself to others without permission from my teacher/parents/carer.
- @ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- @ I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my E-Safety.

@ If I am given a password I never pass it on to anyone, even my best friend.

@ I never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and always report it to my teacher/parents/carer.

@ I never respond to nasty, suggestive or rude e-mails or postings in chat rooms/groups; I always report it to my teacher/parents/carer.

@ I always tell my teacher/parents/carer if I see bad language or inappropriate things while I am online.

@ I am always myself and do not pretend to be anyone or anything that I am not.

@ I know that my school and the Internet service provider will check the sites I have visited.

@ I understand that I will not be able to use the Internet at school if I deliberately misuse it.

@ I understand that all use on a school device is monitored and my screen can be viewed at any time.

@ I understand that if am loaned a school device, I will:

- Always treat it with respect and care.
- Only use the device for school appropriate purposes only.
- Only sign in with my school username and password.
- Only to be used within the hours of 7am to 9pm.

@ I understand that information on the internet may not always be reliable and sources may need checking.

@ I will not login or use any social media sites such as Instagram/Facebook/Twitter or any other age inappropriate site or social media platform.

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times. (Parents are asked to read and explain the rules for responsible use with their children.)

Signed: _____ Class: _____ Date: _____

Parent's Consent for Computer Use and Internet Access

I have read and understood the school Rules for Responsible Internet use and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Print Name: _____ Date: _____

Appendix 2: Acceptable use agreement (Staff, Governors, Volunteers and Visitors)

St Bernadette's Catholic Primary School

ICT Acceptable Use Policy (March 2021)

Teachers, Support Staff and Invited Guests

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

This document outlines the care and procedures staff should take when using ICT, paying special attention to the directives and instructions specified within the 2018 General Data Protection Act (GDPR).

Please read this document carefully.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes.
- Personal devices may connect to the school Wi-Fi guest network only.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.
- Be aware and vigilant of viruses & malware, ensuring to occasionally run scans on equipment (including the school encrypted memory stick)
- If you suspect a virus, malware or hacking, please immediately contact the school's ICT Manager/Support.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Each laptop should be encrypted with BitLocker or equivalent encryption mechanisms, please ensure you have a "padlock" icon present and in the "unlocked" graphic on the C Drive: If this is not the case, please seek support from the ICT Manager immediately and refrain from using the computer outside of the school premises.
- Staff must never use unencrypted memory sticks. All staff are provided with encrypted memory sticks, which must be secured with a strong password.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or the school network at risk.
- Computer storage areas and USB sticks will be treated like school lockers. The ICT Manager, Data Protection Officer or members of the Leadership Team may review your files and communications to ensure that you are using the system responsibly.

- Cameras, iPads and other electronic devices must be securely locked away when not in use.

Password Policy and Access Security

- Passwords must be **strong** and **unique** for each and every login where individuals' data can be accessed. Examples of the latter include, but are not limited to:

  - The computer login
  - Subscription websites such as bugclub, professor assessor, mymaths, etc.
  - SIMS
  - All other sites and programs which store identifiable and sensitive information.

  A strong password is defined as: at least three words, a sentence, or a password made up of at least 10 characters, and must include a number and capital letter(s). e.g. BlueSkyMorning14. DucksAtThePark18.

- Staff members must ensure that they use a different password for each system they use. E.g. SIMS password must be different from the computer login password. Passwords must not be used twice or repeated across different systems.
- Passwords that follow the guidelines of complexity and strength outlined in this document, will not have an enforced policy of change, as per the government guidelines specified here: https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry
- Staff must never leave a laptop unattended without first using CTRL + ALT + DELETE and Enter, to lock the computer.
- Passwords should not be shared. The only exception to this is if you feel it would help the ICT Manager to address IT issues relating to your school account/equipment.
- IPads and other tablets that are taken offsite must be secured by at least a strong 6 digit pin.
- Staff members should be aware that the password used to login to the school computer will also set the Email account password.

Saving Data

- Data residing on the school server will be split into several folders, and must be saved in the appropriate place on the server.
- These areas will be labelled by folder and accessible to staff who have been assigned permissions allowing their use.
- Please ensure data is saved to the correct areas **at all times**. Failure to do so may expose sensitive data to individuals who are not permitted access
- Ensure filenames are appropriately named and do not unnecessarily share data

Drive Types:

- "T Drive" is the main shared drive amongst teachers, supply staff and guests and will contain tiered levels of access depending on access rights.
- "Z Drive" securely contains documents and files relating to safeguarding, and can only be seen/accessed by those privy to sensitive safeguarding material.
- "O" Drive contains files and folders relevant to the Office/SMT & Admin
- "W" Drive is the main shared drive amongst pupils, all pupils and staff are able to see and edit the files in this drive.

Home Access and Computer use outside of school

- Staff will be permitted to use their laptop at home or other private places for work purposes only. This includes access to the school network via the Virtual Private Network (VPN) under the following conditions:

  - Access must only be via the school computer; correctly configured and authorised by the school's ICT Manager and Headteacher/SLT.
  - The computer must be locked before leaving unattended for any amount of time.
  - School equipment must be used extremely vigilantly in public places, or where there is a risk that information could be incidentally or deliberately obtained, either by sight or through connections to unfamiliar networks. The VPN should not be used on public Wi-Fi unless permission has been obtained from the ICT Manager or SLT beforehand.

Printing

- Staff will be required to print all documents with any sensitive information to a photocopier with papercut MF enabled which enforces "Secure Print". Secure print prevents the document printing until the member of staff releases it with a private passcode.
- If Secure Print is not available on any photocopier, staff may print to an 'unsecured' printer, but extreme care must be taken. The member of staff must be stationed next to the destination printer when printing, and ensure all pages are immediately collected.

Discovering and reporting breaches of General Data Protection Regulation (GDPR)

Breaches of data where sensitive information has become obtained by unauthorised individuals (e.g. In plain sight/ on an unlocked computer screen/document left on a printer) etc - must be reported to the Data Protection Officer immediately on discovery of the breach, in line with the schools Data Protection Policy.

It is the responsibility of all members of staff to be constantly vigilant to any breaches of data that may contravene the GDPR.

Internet

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and development of the internet itself.

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

Email & Calendar

St Bernadette's uses Office 365 to process and store Email. As a member of staff, you will have access to this resource. Please familiarise yourself with the following rules around school Email:

- Whenever an email is sent on behalf of the school it should include; the school's name, the sender's name, their job title and email address.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to the ICT Manager. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- Emails should not be loaded onto any personal device.

- Any documents scanned for attachment purposes, must be deleted from the scan folder immediately after being sent.
- Always use your designated school email account for all school related business. Personal email accounts must never be used.
- If you receive an email erroneously sent and it contains sensitive information, please close the email as soon as this is realised and inform the sender immediately, delete and confirm deletion to sender.
- If you believe you have accidentally sent an email to the wrong person or person(s) containing sensitive information, then immediately inform the addressee urgently and instruct them to not read/share/or forward the email and delete immediately. Request confirmation from the recipient that these instructions have been adhered to. All such breaches should be immediately reported to the DPO.
- All email attachments containing sensitive information should be password protected/encrypted with a strong password. The password should be communicated to the recipients verbally where possible, otherwise by a follow up email containing only password.
- Do not include sensitive information with the email body. Ensure this is contained in the attachment only.
- Emails containing sensitive information should not be sent to parents or the public under any circumstances. Please see the school office for communicating such information to parents.
- Internal emails should be void of all sensitive information as far as possible, when needing to include such information, please refer to the location on the school's file server instead of attaching/including in the body of the email.

Social Networking sites

Social media applies to blogs, microblogs such as Facebook, Twitter, Bebo, Linkedin, Videos, social networks, discussion forums, wikis and other personal webspace.

- Social media should not be accessed on the schools premises
- Do not speak for the school unless you have express permission to do so, this covers all comments relating to the school
- If you can be linked to the school, act appropriately. This include photos and status updates
- Remember that colleagues, prospective employers, parents and children may see your online information
- You should not be 'friends' with any pupils from our school. Unless there are exceptional circumstances, e.g. child or sibling
- Please choose your 'friends' carefully, especially in light of the above.
- Ensure your settings are on private and only you and YOUR friends can see them
- If in doubt please seek advice from the school

Disciplinary Action

Disciplinary action may be taken against employees who contravene these guidelines. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the school's acceptable use policy and agree to use the school's computer facilities within these guidelines.

Name: Signature:

Date: