



Remote Learning Policy

Mr D Moss

December 2020

Approved by Chair: _____

Review Date: December 2021

Contents:

[Statement of intent](#)

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Resources](#)
4. [Online safety](#)
5. [Safeguarding](#)
6. [Data protection](#)
7. [Marking and feedback](#)
8. [Health and safety](#)
9. [School day and absence](#)
10. [Communication](#)
11. [Monitoring and review](#)

Statement of intent

At Villiers Primary School, we understand the need to continually deliver quality first education, including during periods of remote working – whether for an individual pupil or many. We recognise the importance of maintaining high expectations in all areas of school life and ensuring that all pupils have access to the learning resources and support they need to succeed.

Through the implementation of this policy, we aim to address the key concerns associated with remote working, such as online safety, access to educational resources, data protection, and safeguarding.

This policy aims to:

- Minimise the disruption to pupils' education and the delivery of the curriculum.
- Ensure provision is in place so that all pupils have access to high quality learning resources.
- Protect pupils from the risks associated with using devices connected to the internet.
- Ensure staff, parent, and pupil data remains secure and is not lost or misused.
- Ensure robust safeguarding measures continue to be in effect during the period of remote learning.
- Ensure all pupils have the provision they need to complete their work to the best of their ability, and to remain happy, healthy, and supported during periods of remote learning.

1. Legal framework

1.1. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Equality Act 2010
- Education Act 2004
- The General Data Protection Regulation (GDPR) 2018
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
- Data Protection Act 2018

1.2. This policy has due regard to national guidance including, but not limited to, the following:

- DfE (2019) 'Keeping children safe in education'
- DfE (2019) 'School attendance'
- DfE (2017) 'Special educational needs and disability code of practice: 0 to 25 years'
- DfE (2018) 'Health and safety: responsibilities and duties for schools'
- DfE (2018) 'Health and safety for school children'
- DfE (2016) 'Children missing education'
- DfE (2020) 'Safeguarding and remote education during coronavirus (COVID-19)'

1.3. This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Special Educational Needs and Disabilities (SEND) Policy
- Behavioural Policy
- Accessibility Policy
- Marking and Feedback Policy
- Curriculum Policy
- Assessment Policy
- Online Safety (e-Safety) Policy
- Health and Safety Policy
- Attendance and Truancy Policy
- ICT Acceptable Use Policy (Appendix 2)
- Staff Code of Conduct
- Data and E-Security Breach Prevention and Management Plan
- Children Missing Education Policy

2. Roles and responsibilities

2.1. The **Governing Body** is responsible for:

- Ensuring that the school has robust risk management procedures in place.
Ensuring that the school has a business continuity plan in place, where required.
- Evaluating the effectiveness of the school's remote learning arrangements.

2.2. The **Head teacher** is responsible for:

- Ensuring that staff, parents and pupils adhere to the relevant policies at all times.
- Ensuring that there are arrangements in place for identifying, evaluating, and managing the risks associated with remote learning.
- Ensuring that there are arrangements in place for monitoring incidents associated with remote learning.
- Overseeing that the school has the resources necessary to action the procedures in this policy.
- Reviewing the effectiveness of this policy on a regular basis and communicating any changes to staff, parents, and pupils.
- Arranging any additional training staff may require to support pupils during the period of remote learning.

- Conducting reviews on a regular basis of the remote learning arrangements to ensure pupils' education does not suffer.

2.3. The **Health and Safety Lead** is responsible for:

- Ensuring that the relevant health and safety risk assessments are carried out within the agreed timeframes, in collaboration with the head teacher.
- Putting procedures and safe systems of learning into practice, which are designed to eliminate or reduce the risks associated with remote learning.
- Ensuring that pupils identified as being at risk are provided with necessary information and instruction, as required.
- Managing the effectiveness of health and safety measures through a robust system of reporting, investigating, and recording incidents.

2.4. The **Data Protection Officer** is responsible for:

- Overseeing that all school-owned electronic devices used for remote learning have adequate anti-virus software and malware protection.
- Ensuring all staff, parents, and pupils are aware of the data protection principles outlined in the GDPR.
- Ensuring that all computer programs used for remote learning are compliant with the GDPR and the Data Protection Act 2018.
- Overseeing that any ICT equipment used for remote learning is resilient and can efficiently recover lost data.

2.5. The **DSL** is responsible for:

- Attending and arranging, where necessary, any safeguarding meetings that occur during the remote learning period.
- Liaising with the **ICT technicians (S4S Rich Robey / John Dalton)** to ensure that all technology used for remote learning is suitable for its purpose and will protect pupils online.
- Identifying vulnerable pupils who may be at risk if they are learning remotely.
- Ensuring that child protection plans are enforced while the pupil is learning remotely, and liaising with the head teacher and other organisations to make alternate arrangements for pupils who are at a high risk, where required.
- Identifying the level of support or intervention required while pupils learn remotely and ensuring appropriate measures are in place.
- Liaising with relevant individuals to ensure vulnerable pupils receive the support required during the period of remote working Ensuring all safeguarding incidents are adequately recorded and reported.

2.6. The **SENCO** is responsible for:

- Liaising with the ICT technicians to ensure that the technology used for remote learning is accessible to all pupils and that reasonable adjustments are made where required.
- Ensuring that pupils with EHC plans continue to have their needs met while learning remotely, and liaising with the head teacher and other organisations to make any alternate arrangements for pupils with EHC plans and IHPs.
- Identifying the level of support or intervention that is required while pupils with SEND learn remotely.
- Ensuring that the provision put in place for pupils with SEND is monitored for effectiveness throughout the duration of the remote learning period.

2.7. The **Office Manager** is responsible for:

- Arranging the procurement (in collaboration with the Computing Lead and ICT Technicians) of any equipment or technology required for staff to teach remotely and for pupils to learn from home.
- Ensuring value for money when arranging the procurement of equipment or technology.
- Ensuring that the school has adequate insurance to cover all remote working arrangements.

2.8. The **ICT technicians (S4S Rich Robey / John Dalton)** are responsible for:

- Ensuring that all school-owned devices used for remote learning have suitable anti-virus software installed, have a secure connection (VPN), can recover lost work, and allow for audio and visual material to be recorded, where required.
- Ensuring that any programs or networks used for remote learning can effectively support a large number of users at one time, where required, e.g. undertaking 'stress' testing.
- Working with the **SENCO** to ensure that the equipment and technology used for learning remotely is accessible to all pupils and staff.

2.9. **Staff members** are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Reporting any health and safety incidents to the **health and safety officer** and asking for guidance as appropriate.
- Reporting any safeguarding incidents to the **DSL** and asking for guidance as appropriate.
- Taking part in any training conducted to meet the requirements of this policy, including training on how to use the necessary electronic equipment and software.
- Reporting any dangers or potential dangers, they identify, as well as any concerns they may have about remote learning, to the **headteacher**.

- Reporting any defects on school-owned equipment used for remote learning to an **ICT technician**.
- Adhering to the Staff Code of Conduct at all times.

2.10. **Parents** are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring their child is available to learn remotely at the times set out in paragraphs [9.1](#) and [9.2](#) of this policy, and that the schoolwork set is completed on time and to the best of their child's ability.
- Reporting any technical issues to the school as soon as possible.
- Ensuring that their child always has access to remote learning material during the times set out in paragraphs [9.1](#) and [9.2](#).
- Reporting any absence in line with the terms set out in paragraph [9.6](#).
- Ensuring their child uses the equipment and technology used for remote learning as intended.
- Adhering to the **Parent Code of Conduct** at all times.

2.11. **Pupils** are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring they are available to learn remotely at the times set out in paragraphs [9.1](#) and [9.2](#) of this policy, and that their schoolwork is completed on time and to the best of their ability.
- Reporting any technical issues to **their teacher** as soon as possible.
- Ensuring they have access to remote learning material and notifying a responsible adult if they do not have access.
- Notifying a responsible adult if they are feeling unwell or are unable to complete the schoolwork they have been set.
- Ensuring they use any equipment and technology for remote learning as intended.
- Adhering to the Behavioural Policy at all times.
- Report all online contact to parents or carers.

3. Resources

Learning materials

3.1. For the purpose of providing remote learning, the school may make use of:

- Work booklets
- Printed material
- Email
- Past and mock test papers
- Online learning portals
- Educational websites

- Reading tasks
- Pre-recorded video or audio lessons

The School's Online Offer:

Villiers Primary School will provide secure access to the **Microsoft TEAMS** platform for children in **Reception through to Year 6**, to share online work. It is compatible with a wide range of digital devices, including laptops, tablets and smart phones. All pupils will be provided a secure username and password (available through the school office). Teachers will upload curriculum-relevant work each day as an assignment with supporting material available in the files section. Work provided will total a minimum of 3 hours' worth of work for each child daily covering at minimum Maths, English and one other subject. Pupils' submitted work will be recognised daily with detailed feedback given at least once per week. Private messaging of any form is not permitted through the TEAMS platform, between pupils and teachers. A public 'message board' is provided for wider contact between staff and pupils for the purposes of supporting with work. All documents submitted by and to staff are accessible by the system administrator. Work will be set using the assignments feature of the TEAMS system. A crib sheet will be provided to children and parents (Appendix 1) to enable children to access the work on the platform. Children, as part of the Microsoft subscription, also have access to the Microsoft Office Suite available through portal.office.com and within TEAMS. Set work will always be saved in file formats which can be accessed by the children (namely, .docx, .pptx, .xlsx, .pdf .jpeg). For those children in **Nursery**, work and activities will be provided via **MarvellousME** with parents/carers provided with an individualised access code and instructions. Parents and carers will submit work back to staff via the Nursery email system:
ContactVilliersNursery@villiersprimaryschool.co.uk

The '**Purple Mash**' Learning Platform is an award-winning cross-curricular website for nursery and primary school children. It enables children to explore and enhance their knowledge in a fun and creative way. Villiers Primary will provide (via the school office) all pupils with a secure username and password. This interactive website will provide additional curriculum enrichment activities to further support out of school learning across a range of digital devices and form part of the enrichment opportunities children have access to through the Computing curriculum at Villiers.

Times Tables Rock Stars is a carefully sequenced programme of daily times tables practice. Villiers Primary School will provide pupils with a secure username and password (via the school office). This will allow interactive times table practice as directed by the class teacher.

All online resources are accessible through a wide range of Internet connected devices and are not platform dependant (e.g. only Mac or Android).

The School's offline offer:

Villiers will provide paper-based learning packs to pupils via the school office. Contact should be made with the school office to access this service and prior notice given.

- 3.2. Teachers will review the DfE's list of [online education resources](#) and evaluate and utilise these tools as necessary, in addition to existing resources.
- 3.3. Reasonable adjustments will be made to ensure that all pupils have access to the resources needed for effective remote learning.
- 3.4. Lesson plans will be adapted to ensure that the curriculum remains fully accessible via remote learning, where practical. Where this is not practical, the school will ensure pupils can catch up on these areas of the curriculum when they return to school.
- 3.5. Teaching staff will liaise with the **SENCO** and other relevant members of staff to ensure all pupils remain fully supported for the duration of the remote learning period.
- 3.6. Any defects or issues with remote learning resources will be reported as soon as possible to the relevant member of staff.
- 3.7. Pupils will be required to use their own or family-owned equipment to access remote learning resources, unless the school agrees to provide loan equipment, e.g. laptops. Some outside agencies may provide digital equipment; details and eligibility will be announced as schemes become available.
- 3.8. Pupils and parents will be required to maintain the upkeep of any equipment they use to access remote learning resources.
- 3.9. Teaching staff will oversee academic progression for the duration of the remote learning period and will mark and provide feedback on work in line with [section 7](#) of this policy.
- 3.10. The **ICT technicians** are **not** responsible for providing technical support for equipment that is not owned by the school.

Food provision

- 3.11. The school will signpost parents via online social media, text or letter towards additional support for ensuring their children continue to receive the food they need, e.g. food banks.

3.12. Where applicable, the school may provide the following provision for pupils who receive FSM:

- Making food hampers available for delivery or collection
- Providing vouchers to families

Costs and expenses

3.13. The school will not contribute to any household expenses incurred while pupils learn remotely, e.g. heating, lighting, or council tax.

3.14. The school will not reimburse any costs for travel between pupils' homes and the school premises.

3.15. The school will not reimburse any costs for childcare.

3.16. If a pupil is provided with school-owned equipment, the responsible adult of the pupil will sign and adhere to the **Acceptable Use Policy** (Appendices 2 & 3) prior to commencing remote learning. Records of these will be maintained in the school office.

4. Online safety

4.1. This section of the policy will be enacted in conjunction with the school's **Online Safety Policy (e-Safety)**.

4.2. Where possible, all interactions will be textual and public.

4.3. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school in line with the Behaviour Policy.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable Internet and WiFi connection to avoid disruption.
- Always remain aware that they are visible.

4.4. All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.

- Not record, store, or distribute audio material without permission.
 - Ensure they have a stable Internet and WiFi connection to avoid disruption.
 - Always remain aware that they can be heard.
- 4.5. The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the **SLT**, in collaboration with the **SENCO**.
- 4.6. Pupils not using devices or software as intended will be disciplined in line with the **Behaviour Policy**.
- 4.7. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.
- 4.8. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.
- 4.9. The school will communicate to parents about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology.
- 4.10. During the period of remote learning, the school will maintain regular contact with parents to:
- Reinforce the importance of children staying safe online.
 - Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
 - Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
 - Direct parents to useful resources to help them keep their children safe online.
- 4.11. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

5. Safeguarding

- 5.1. This section of the policy will be enacted in conjunction with the school's **Child Protection and Safeguarding Policy**, which has been updated to include safeguarding procedures in relation to remote working.

- 5.2. The **DSL** and **head teacher** will identify 'vulnerable' pupils (pupils who are deemed to be vulnerable or are at risk of harm) via risk assessment prior to the period of remote learning.
- 5.3. The **DSL** will arrange for regular contact to be made with vulnerable pupils, prior to the period of remote learning.
- 5.4. Phone calls made to vulnerable pupils will be made using school phones where possible.
- 5.5. The **DSL** will arrange for regular contact with vulnerable pupils **once** per **week** at minimum initially, with additional contact, including home visits, arranged where required. This provision will be reviewed on a weekly basis and may be subject to change.
- 5.6. All contact with vulnerable pupils will be recorded on paper and suitably stored in line with the records management procedures.
- 5.7. The **DSL** will keep in contact with vulnerable pupils' social workers or other care professionals during the period of remote working, as required.
- 5.8. All home visits **must**:
- Have at least **one** suitably trained individual present.
 - Be undertaken by no fewer than **two** members of staff.
 - Be suitably recorded on paper or CPOMS and the records stored so that the **DSL** has access to them.
 - Actively involve the pupil.
- 5.9. Vulnerable pupils will be provided with a means of contacting the **DSL**, their deputy, or any other relevant member of staff – this arrangement will be set up by the **DSL** prior to the period of remote learning. In most cases, this will be the provision of a phone number, email or direct messaging contact.
- 5.10. The **DSL** will meet (in person or remotely) with the relevant members of staff **once** per **month** through Case Sharing meetings to discuss new and current safeguarding arrangements for vulnerable pupils learning remotely.
- 5.11. All members of staff will report any safeguarding concerns to the **DSL** immediately.
- 5.12. Pupils and their parents will be encouraged to contact the **DSL** if they wish to report safeguarding concerns, e.g. regarding harmful or upsetting content or incidents of online bullying. The school will also signpost families to the practical support that is available for reporting these concerns.

6. Data protection

- 6.1. This section of the policy will be enacted in conjunction with the school's **Data Protection Policy**.
- 6.2. Staff members will be responsible for adhering to the **GDPR** when teaching remotely and will ensure the confidentiality and integrity of their devices at all times.
- 6.3. Sensitive data will only be transferred between devices if it is necessary to do so for the purpose of remote learning and teaching.
- 6.4. Any data that is transferred between devices will be suitably encrypted or have other data protection measures in place so that if the data is lost, stolen, or subject to unauthorised access, it remains safe until recovered.
- 6.5. Parents' and pupils' up-to-date contact details will be collected prior to the period of remote learning.
- 6.6. All contact details will be stored in line with the **Data Protection Policy** and retained in line with the **Records Management Policy**.
- 6.7. The school will not permit paper copies of contact details to be taken off the school premises.
- 6.8. Pupils are not permitted to let their family members or friends use any school-owned equipment which contains personal data.
- 6.9. Any breach of confidentiality will be dealt with in accordance GDPR procedures and will be discussed with the DPO as necessary
- 6.10. Any intentional breach of confidentiality will be dealt with in accordance with the school's **Behavioural Policy** or the **Disciplinary Policy and Procedure**.

7. Marking and feedback

- 7.1. All schoolwork set through remote learning must be:
 - Complete when returned to the relevant member of teaching staff.
 - Returned before the deadline set by the relevant member of teaching staff.
 - Completed to the best of the pupil's ability.
 - The pupil's own work.
 - Returned with feedback using the TEAMS feedback function.
- 7.2. The school expects pupils and staff to maintain a good work ethic and a high quality of work during the period of remote learning.
- 7.3. Pupils are accountable for the completion of their own schoolwork – teaching staff will contact parents via the school office if their child is not completing their schoolwork or their standard of work has noticeably decreased.

- 7.4. Pupils will be excused work for genuine reasons.
- 7.5. Teaching staff will monitor the academic progress of pupils with and without access to the online learning resources and discuss additional support or provision with the **head teacher** as soon as possible.
- 7.6. Teaching staff will monitor the academic progress of pupils with SEND and discuss additional support or provision with the **SENCO** as soon as possible.

8. Health and safety

- 8.1. This section of the policy will be enacted in conjunction with the school's **Health and Safety Policy**.
- 8.2. Teaching staff and **ICT technicians** will ensure pupils are shown how to use the necessary equipment and technology safely and correctly prior to the period of remote learning.
- 8.3. If using electronic devices during remote learning, pupils will be encouraged to take a screen break every hour.

9. School day and absence

- 9.1. Pupils will be present for remote learning from **Monday** to **Friday**, with the exception of breaks and lunchtimes, as outlined in paragraph 9.2.
- 9.2. Breaks and lunchtimes will take place at appropriate times.
- 9.3. Pupils are not expected to do schoolwork during the times outlined in paragraph 9.2.
- 9.4. Pupils with SEND or additional medical conditions who require more regular breaks, e.g. sensory breaks, are not expected to do schoolwork during their breaks.
- 9.5. Pupils who are unwell are not expected to be present for remote working until they are well enough to do so.

10. Communication

- 10.1. The school will ensure adequate channels of communication are arranged in the event of an emergency.
- 10.2. The school will communicate with parents via social media, text, website or letter about remote learning arrangements.
- 10.3. The **SLT** will communicate with staff as soon as possible via email about any remote learning arrangements.

- 10.4. Members of staff involved in remote teaching will ensure they have a working device that is available during their agreed working hours.
- 10.5. The school understands that pupils learning remotely have the right to privacy out-of-hours and should be able to separate their school and home lives – communication is only permitted during school hours.
- 10.6. As much as possible, all communication with pupils and their parents will take place within the school hours outlined in [section 9](#).
- 10.7. Pupils will have the opportunity for verbal contact with a member of teaching staff, during the period of absence.
- 10.8. Parents and pupils will inform the relevant member of staff as soon as possible if schoolwork cannot be completed.
- 10.9. Issues with remote learning or data protection will be communicated to the **school office** as soon as possible so they can investigate and resolve the issue.
- 10.10. The **pupils' teacher** will keep parents and pupils informed of any changes to the remote learning arrangements or the schoolwork set.
- 10.11. The **Head teacher** will review the effectiveness of communication on a regular basis and ensure measures are put in place to address gaps or weaknesses in communication.

11. Monitoring and review

- 11.1. This policy will be reviewed on an **annual** basis by the **SLT & Computing Lead**.
- 11.2. Any changes to this policy will be communicated to all members of staff and other stakeholders.
- 11.3. The next scheduled review date for this policy is December 2021.

Appendix 1

Villiers Primary School
Prouds Lane, Wolverhampton
WV14 6PR, 01902 558993
Updated 18.11.20

Work hard. Be kind.

Villiers Primary School



Microsoft Teams

Home Learning Crib Sheet (Pupils Rec & Years 1-6)

In the case of online home learning having to take place, please use the following guide to help you access our online learning system, Microsoft Teams. We recommend you try and log in soon to ensure that, in the case of your child having to use the system, you and your child will be familiar with the process.

As part of the subscription, your child will have access to the Microsoft Office Suite so work can be completed electronically if you cannot print the work.

To access Microsoft Teams, go to:

teams.microsoft.com

or download the Microsoft Teams app to your laptop or device:



In order to login, complete the Username and Password fields:

Username:

@villiersprimaryschool.co.uk

Password:

Once you are logged in, navigate to the '**General**' Channel and locate the '**Assignments**' tab.

This is where children can access work set for them. The files uploaded are read-only and therefore children can only download work from this location. Children will need to upload work by clicking the '**Add Work**' link and browsing their device for the file. Once they have uploaded their work or evidence for that assignment, press the '**Turn In**' option. Once turned in, children can edit their document until the submission date expires. Teachers will review work submitted and comment back via the feedback option.

Children will be prompted under the '**activity**' tab for any work they haven't completed or for any new work set. A red dot like a notification will also be present.

Remember you also have access to Microsoft Office which can be accessed via portal.office.com and logging in.

Many thanks for your continued support.

Appendix 2

Villiers Primary School
Prouds Lane, Wolverhampton
WV14 6PR, 01902 558993
Updated 14.11.19

Work hard. Be kind.

Villiers Primary School

Acceptable Use Policy



Date of Policy: 14th November 2019

Date of Review: 14th November 2022

Introduction

It is the responsibility of all users of the University of Bath's I.T. services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.1 Purpose

This Acceptable Use Policy (AUP) is intended to provide a framework for such use of the School's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.2 Policy

This AUP is taken to include the Data Protection Policy and the GDPR Regulation. The school also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

1.3 Scope

Members of Villiers Primary School and all other users (staff, students, visitors, contractors and others) of the school's facilities are bound by the provisions of its policies in addition to this AUP. Villiers Primary School seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the wider Academy Trust.

2 Unacceptable Use

a) Subject to exemptions defined in 2f), the School Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited "nuisance" emails;
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the School, Trust or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings the Villiers Primary School or Shine Academies into disrepute.

b) The School Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. intentionally wasting staff effort or other School resources;
2. corrupting, altering or destroying another User's data without their consent;
3. disrupting the work of other Users or the correct functioning of the School Network;
4. denying access to the School Network and its services to other users;
5. pursuance of commercial activities (even if in support of school business), subject to a range of exceptions.

c) Any breach of industry good practice that is likely to damage the reputation of the school will also be regarded prima facie as unacceptable use of the School Network.

d) Where the School Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the School Network.

e) Users shall not:

1. introduce data-interception, password-detecting or similar software or devices to the School's Network;
2. seek to gain unauthorised access to restricted areas of the School's Network;
3. access or try to access data where the user knows or ought to know that they should have no access;
4. carry out any hacking activities; or
5. intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

f) Exemptions from Unacceptable Use: There are a number of legitimate academic activities that may be carried out using School information systems that could be considered unacceptable use, as defined at 2a-e. For example, research involving defamatory, discriminatory or threatening material or language, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques. In such circumstances, advice should be sought from the School's Head Teacher.

3 Consequences of Breach

In the event of a breach of this AUP by a User, the School may in its sole discretion:

- a) restrict or terminate a User's right to use the School Network;
- b) withdraw or remove any material uploaded by that User in contravention of this Policy; or
- c) where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the User is also a member of the School community, the School may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Charter, Statute, Ordinances and Regulations.

4 Definitions

School Network – all computing, telecommunication, and networking facilities provided by the School, with particular reference to all computing devices, either personal or owned, connected to systems and services supplied.

updated 14th November 2019 by D Moss (IT Curriculum Leader)

reviewed 15th November 2019 by L Westwood (Head Teacher)

Appendix 3

Villiers Primary School
Pondside Lane, Mallowhampton
Wiltshire, SN10 6JH
Updated 18.12.20

Work hard. Be kind.

Villiers Primary School Laptop Loan Agreement



By accepting and signing this document, I agree to the following:

- The Laptop, bag, power supply and router (if applicable) remain the sole property of the Department for Education (DfE).
- I acknowledge that the laptop is monitored by the DfE using Microsoft Intune and data is collected in line with their GDPR statement.
- The School is acting as an agent who is overseeing the distribution and collection of devices.
- I will adhere to the school's Acceptable Use Policy and associated documentation.
- I will return and surrender any loaned equipment to the school on the date advised.
- The Laptop, bag, power supply and router (if applicable) will **ONLY** be used for the purposes of home learning by the assigned student.
- I am responsible at all times for the equipment and confirm that this is covered on my home insurance and, if applicable, car insurance.
- I recognise that I am responsible for any damage to the equipment.

Name of child:

Name & Signature (parent/carer):

Start Date of Loan:

Return Date:

Laptop Serial Number:
