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)