Acceptable Use Policy: Staff

Northgate Primary School

Approved by:	Northgate Governing Body
Last reviewed on:	March 2026
Next review due by:	March 2027

School networked resources, including Dojo and Tapestry, are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. If you make a comment about the School or County Council, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the School or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services and, in some instances, could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Head Teacher.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos / code of conduct.

Internet and Computing Rules	
1.	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any person or bring the school (or West Sussex County Council) into disrepute.
2.	I will use appropriate language – I will remember that I am a representative of the school and not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
3.	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
4.	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
5.	I will not trespass into other users' files or folders.
6.	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself. Likewise, I will not share those of other users.

7.	I will ensure that, if I think someone has learned my password, then I will change it immediately and/or contact IT Support (Virtual IT).
8.	I will ensure that I log off after my network session has finished.
9.	If I find an unattended machine logged on under another user's username, I will **not** continue using the machine – I will log it off immediately. I should notify the previous user of this and remind them of the best practice on logging out after finishing a session.
10.	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school.
11.	I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
12.	I will not use the network in any way that would disrupt use of the network by others.
13.	I will report any accidental access, receipt of inappropriate materials or filtering breaches / unsuitable websites to the Head Teacher who at their discretion will contact IT Support (Virtual IT).
14.	I will not use USB drives, portable hard drives, tablets or personal laptops on the network without having them approved by the school and checked for viruses.
15.	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
16.	I will not download any unapproved software, system utilities or resources from the internet that might compromise the network or are not adequately licenced.
17.	I will not accept invitations from children and young people to add me as a friend to their social networking sites, not will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such as school parents and their children.
18.	I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role in any way.
19.	I will complete the Secure Schools Cyber Training
20.	I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the internet and related technologies.
21.	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held in Bromcom.

22.	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using video conferencing or web broadcasting.
23.	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24.	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25.	I will ensure that any personal data (where the Data Protection Act applies) that is sent over the internet (or taken off site in any other way) will be encrypted or otherwise secured.
26.	If I feel that I have caused a data breach by sending or losing personal data, I will contact the DPO straight away with all of the information to aid the DPO
27.	I have read and signed the data protection policy.
28.	I will not use or download any school apps on home devices or mobiles and only use them on secure school devices including but not limited to Bromcom, CPOMS, Dojo, Tapestry or SCOPAY. Only in emergencies like a security breach should these be accessed via a mobile phone with the consent of the Head Teacher.
29.	Any information regarding children or relating to school should only be discussed via Teams and Team Chats only. Private messaging groups (e.g. WhatsApp) should only be used for personal or social use.
30.	I will not voluntarily give my mobile phone to family or children, as this may give them access to secure information such as my school email.
31.	I will alert the Head Teacher and DPO immediately if any electronic devices (including personal mobile phones) are lost or stolen.
32.	My electronic devices, including personal mobile phones, will be locked and protected using face ID, fingerprint or password.
33.	I will not store school information including photos on personal devices.
34.	Two-factor authentication is required on school email accounts, and I will take the necessary steps to set this up. Where available, I will enable two-factor authentication on any system that contains school data.
35.	If I notice or am made aware of any suspicious activity on school equipment or accounts (such as spoof emails, encrypted files, unusual file names or unauthorised access), I will contact Virtual IT (via 01903 767122) and a member of SLT immediately.

Additional guidelines

- Staff must comply with the Acceptable Use Policy of any other networks that they access.
- Staff will follow the "Safer Use of the Internet by Staff Working With Young People" published within the West Sussex Schools Acceptable Use Policy; http://wsgfl.westsussex.gov.uk/AUP

SERVICES

There will be 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 damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are to call IT Support immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by IT Support. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

Further guidance can be found in the "Model Policy for schools regarding photographic images of children" August 2010.

Copies can be obtained from section 5 of the WSCC Schools Acceptable Use Policy; http://wsgfl.westsussex.gov.uk/AUP

NORTHGATE PRIMARY SCHOOL

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school's Acceptable Use Policy. If I am in any doubt I will consult the Head Teacher or DPO.

I agree to report any misuse of the network to the Head Teacher.

I also agree to report any websites that are available on the school internet that contain inappropriate material to the Head Teacher.

Lastly, I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the Head Teacher.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: _____

Staff Signature: _____

Date: ____ / ____ / _____