



St. Nicholas  
S c h o o l

## Acceptable Use of ICT Policy

St Nicholas School is working towards the UNICEF Rights Respecting School Award and promotes rights respecting values in all its policies



The Governing Board of St Nicholas School formally adopted this Policy  
on 14<sup>th</sup> October 2021

To be reviewed October 2022

Signed

  
\_\_\_\_\_

Headteacher

Signed

  
\_\_\_\_\_

Chair of Governors

## St Nicholas - Staff Acceptable Use of ICT Policy



School networked resources, including the London Grid for Learning and Learning Platforms 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 Croydon 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 Croydon Council into disrepute is not allowed and subject to sanction via the code of conduct / discipline policy.

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

### CONDITIONS OF USE

#### 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's Data Protection / E-Security Policies, The Data Protection Act 2018 and the school ethos.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or Croydon Council) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the school on a global public system such as Facebook. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	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.

5	GDPR – 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.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users. I will ensure that I follow the E-Security Policy for Password updates.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the Head Teacher.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username I will <b>not</b> continuing using the machine – I will log it off immediately and inform the DPCO of the Data Breach.
11	I will not use <b>personal</b> digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I understand that I am <b>prohibited</b> from using any email address except the lgfl account allocated to me by St Nicholas School. I must use this for all school correspondence.
13	I am aware that e-mail 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.
14	I will not use the network in any way that would disrupt use of the network by others.
15	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the Head Teacher.
16	I will not use "USB drives", portable hard-drives, "floppy disks" or personal laptops on the network.
17	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.
18	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
19	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.  As damage to professional reputations can inadvertently be caused by quite innocent postings or images on web pages or social networking sites - 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 a school parents and their children.
20	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.

21	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.
22	I will not send or publish material that violates Data Protection Act (GDPR) 2018 or breaching the security this act requires for personal data, including data held on the SIMS Learning Gateway.
23	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
24	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
25	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, whether at school, in my home or journey between.
26	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.
27	I will abide by the school's E-Security Policy / Data Protection (GDPR) policy at all times.
28	I understand that <b>I must not access</b> my mobile phone during my working day, except when at break / lunch for personal use. I understand may use my phone to access school software e.g. WEDUC / emails etc when necessary. Please speak to the Head Teacher or the Deputy Head of your KS if you need to keep your phone with you during school time for emergency family reasons.
29	You can use your mobile to contact the school / emergency services etc while on school trips / off site.

### **Additional guidelines**

- Staff must comply with the acceptable use policy of any other networks that they access.

### **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 expected to inform the Head Teacher 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 the school's ICT Support contractors' / school ICT staff and SLT. Users identified as a security risk will be denied access to the network.

### **MEDIA PUBLICATIONS**

The school's holds documents that indicate whether a pupil's parent / carer has given permission for photographs with or without names can be 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.