Internet Access Policy

Networked resources, including Internet access, are potentially available to students and staff in the school. All staff are required to follow the conditions laid down in this 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.

Networked resources are intended for educational purposes, including administrative work, and may only be used for legal activities consistent with the rules of St Nicholas School. Any expression of a personal view about the school or Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or Croydon Council into disrepute is not allowed.

St Nicholas School expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources.

Unsupervised pupil use of the Internet or
St Nicholas' school network is not allowed

All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Conditions of Use
Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff, and pupils, will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the ICT Coordinator and / or senior management.

Misuse of the Internet service provided by the School includes but is not limited to:

- Searching for or making, sending, displaying or publishing any material (e.g. imagery, sound or information) that is likely to cause offence, inconvenience, needless anxiety and/or bring the school into disrepute.
- Searching for / looking at, making or publishing offensive material.
- Receiving, publishing or sending material that breaks Copyright Law or the Data Protection Act.
- Sending unsolicited material to other users (including those on other networks)
- Trying to look at data and resources on the school office network system or other systems outside school unless permission has been granted.
- Acting in a way that would cause corruption or destruction of other users' data, violate the privacy of other users or intentionally waste time or resources on the school system or elsewhere.
- Downloading software without the approval of the *member of staff responsible*.
- Spending excessive amounts of time using the Internet for non-school/work related reasons. (Incidental personal use is permitted provided it complies with these protocols and does not interfere with work or study).

Failure to adhere to these protocols may result in loss of access to the Internet as well as other disciplinary action.

Other Considerations

- Being polite and never sending, or encouraging others to send, abusive messages. Defamatory comments could result in legal action. E-mail has been used successfully as evidence in libel cases.
- Using appropriate language. Users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- 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 should not be sent. The school reserves the right to apply monitoring arrangements in relation to e-mail use where misuse is suspected.
- Not using the Internet in any way that would disrupt the use of the network by others. The school reserves the right to apply monitoring arrangements to any student or member of staff in relation to Internet use and related services where misuse is suspected.

The Purpose of Monitoring or the Investigation of Users

- To ensure compliance with the schools Acceptable Use Policy
- To investigate unauthorised use of the Internet and e-mail systems.
- To protect the operational availability and performance of ICT technical infrastructure.
- To continue the work of a school if an addressee is absent.
- To comply with the County Council's statutory obligations.
- To prevent or detect crime.

Filtering

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Croydon Council can accept liability for the material accessed, or any consequences of Internet access. St Nicholas School must gain parental permission before pupils are able to access the Internet.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Internet content. Filtering may be performed by:

- Internet Service Provider
- Croydon Council
- School-level systems or
- any combination of the above

By default a Primary or Secondary filter is automatically in place for Croydon schools using the Atomwide services.

School-level systems require considerable management to maintain effectiveness and place huge responsibility on the school if they are the only systems in place.

Careful monitoring and management of all filtering systems will be required. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

Action for Schools - Filtering

- The school will work in partnership with parents, the local authority, DfES and the Internet Service Provider to ensure that the Internet filter systems protect pupils and are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (website address) and content must be reported to the Internet Service Provider via the nominated contact / ICT Coordinator
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Headteachers having reasonable suspicion that a member of staff is misusing the system may consult with their HR Business Partner to obtain guidance before instigating an investigation into e-mail or Internet Access misuse.
- **Ratified by the Governing Body**
-
-
- **Signed……. Chair of Governors**
-
- **Signed ……. Head Teacher**
-
- **Date ……**