

INTERNET USAGE POLICY

De Lacy Academy monitors all Internet activity of users for the purposes of providing safe Internet access. Information recorded as part of this automated monitoring process includes user identification, computer address, domain names of websites visited and blocked, duration, date and time of visits, and URLs of files and objects requested, blocked and downloaded from the Internet.

Privacy:

Users must be aware that monitoring may reveal sensitive data about them, for example visits to websites which details the activities of a particular political party or religious group might indicate the political opinion or religious belief of that staff member, or self-help or health advice sites might identify a physical or mental health condition.

By accepting the usage and monitoring policy when logging into and carrying out such activities using The De Lacy Academy School Network, all users consent to the school processing any sensitive personal data about them; this may be revealed through monitoring.

All monitoring data collected will be kept secure and private within the system and its use compliant with UK access monitoring and reporting laws.

Sharing of monitoring data with third parties:

- Monitoring data may be shared with Wakefield Council as part of their duties as the Local Education Authority and with The School Partnership Trust.
- Monitoring data may be shared with the British Educational Communications and Technology Agency (BECTA) and the Department for Children, Schools and Families (DCSF).
- Following receipt of formal requests, specific monitoring data may be shared with the Police or other UK government authorities to assist their enquiries.

Monitoring Data Retention Policy:

- Monitoring data stored and archived within The De Lacy Academy School systems will be retained for a maximum period of 12 months and then be destroyed.
- Monitoring data supplied to the departments above will be retained according to their respective Data Protection Statements.

Acceptable Use Policy

- Users shall have regard to the varying laws which have an impact of the use of such facilities. Such laws include (but are not limited to) The Data Protection Act 1998, The Defamation Act 1996, The Obscene Publications Act 1964, The Computer Misuse Act 1990, The Copyright, Designs and Patents Act 1998 and The Human Rights Act 1998.
- You must not create, copy or exchange information which belongs to someone else in contravention of copyright or other intellectual property laws (such as music, video or software).
- You must not use network facilities to threaten, bully, coerce, abuse, groom, spoof or fraudulently obtain information or goods. You must not use the school network for trade or personal gain.

E-mail Policy

- In-coming and outgoing e-mail will be regarded as public and will be monitored. Systems are in place to automatically detect and block infected emails as well as SPAM (Self Promoting Advertising Messages).
- The forwarding of chain letters will be banned, as will the use of chat lines.
- You must not use email to broadcast or forward malicious software, obscenities, advertisements, or other unsolicited content.
- The sending of any sensitive personal data, for example home address, photographs or personal telephone numbers relating to the user or any other person is forbidden.
- Users will be held responsible for e-mail sent from their account.

Internet Access Filtering and Blocking

- Individuals are responsible for their account and password security.
- Some example filtering categories are:
 - Pornographic, Adult, Tasteless or Offensive Material
 - Violence (including Weapons and Bombs)
 - Racist, Extremist and Hate Material
 - Illegal Drug Taking and Promotion
 - Criminal Skills and Software Piracy
- Supervision
- The automated filtering systems used are aware of more than one billion unsuitable URL's, however, no automated filtering system can be completely effective on its own and a combination of approaches is needed. It is acknowledged that adequate supervision is essential, especially when minors are using the Internet.