

Woodthorpe J.I. School

Acceptable Use of School Digital Technology and the Internet Policy for Adults

This policy outlines the acceptable use of emerging technologies in school and explains how our school is seeking to avoid the potential problems for staff that unrestricted Internet access could give rise to.

Internet access in school

The purpose of Internet access in schools is to raise educational standards, support the professional work of staff and enhance the school's management, information and business administration systems.

Teachers will have access to web sites worldwide (including museums and art galleries) offering educational resources, news and current events.

In addition, staff will have the opportunity to access educational materials and good curriculum practice; to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA and DfE; and receive up-to-date information.

Maintaining the security of the school ICT network

Security is maintained by providing automatically updated virus protection.

Acceptable Internet Use

The computer network and laptops are owned by the school, and may be used by staff to enhance their professional activities including teaching, research, administration and management. The school's Acceptable Use Policy for Adults has been drawn up to protect all parties – the children, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Internet Usage on the school network and laptops is monitored by a LA endorsed software system (Policy Central) that searches for inappropriate words and phrases including those related to radicalization and terrorist activities. Reports of any found will be generated by the LINK2ICT and returned to the school. As a result of this messages may be blocked and sites with unsuitable content will be blocked.

- All Internet activity should be appropriate to staff professional activity or the children's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Users are responsible for all e-communication sent and for contacts made that may result in e-communication being received;
- Personal electronic account information, e.g. e-mail addresses, must not be given to children.
- Personal electronic account information, e.g. e-mail addresses, must not be accessed from school equipment.

- Use of school ICT equipment for personal financial gain, gambling, political purposes, advertising, to access inappropriate materials such as pornographic, racist, radicalisation or offensive material, will result in disciplinary action.
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- The use of public chat rooms and social networking sites is not allowed.
- As E-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- If You Tube is used the video window should be maximized to avoid children viewing any unsuitable surrounding content.
- For safeguarding purposes staff must never disclose information about the school, the children, parents, governors, members of staff or other stakeholders on social networking sites such as Facebook. Facebook must not be used in school and is blocked by Policy Central. Except for where using an agreed and approved communication channel on behalf of the school e.g. Woodthorpe J.I Twitter account.
- For safeguarding purposes staff must never disclose their personal telephone numbers, email address or social network usernames to pupils.

Laptops and I pads

- Staff need to be aware that laptops and I pads are not insured if they are accidentally damaged or stolen by means of forced entry or assault. If taken from a staff members home, a claim should be made from their home insurance.
- If a laptop or I pad has been stolen the police need to be notified and a crime reference obtained.
- Staff need to be vigilant about where they store their laptop or I pad in school.
- Laptops and I pads will not be covered whilst in transit or left unattended in a vehicle. If taken from a staff member's car, a claim should be made on the car insurance.
- Laptops must only be connected to the internet at home through a firewall.
- Laptops and I pads must be signed for and the serial number recorded before they are taken out of school.
- Memory sticks must not contain information about school children, parents, Governors or members of staff.
- The use of personal devices on the School's wireless network is not permitted

School Cameras

- Photographs taken in school will be taken on school cameras and I pads. The content should be processed in school.
- Staff must obtain the permission of the Head teacher, Deputy Head teacher or Designated Senior Person (DSP) for Child Protection to work on materials at home.
- Staff taking images of children must adhere to the 'Use of Images of Children' policy. A list of parental permissions for publishing images of their children is kept in the school office and updated on an ongoing basis. Staff are responsible for checking that they have the most recent parental permissions before publishing images.

Mobile Phones

- Mobile phones should not be used for personal calls or texting in teaching time except in the event of an emergency.
- Personal mobile phone numbers must not be given to pupils.
- Mobile phones must not be used for taking photographs.
- Personal mobile phones must be switched off or on silent during teaching time.

- Any adult in school who finds an inappropriate image on a mobile phone in school must report this immediately to a DSL. That adult must not look at, send on or print the image.. All staff will respond to incidents of sexting, using our procedures which are updated according to the latest advice from J. Needham, LSCB.

Training

- Members of the E. Safety Committee will keep up to date by attending training about E.Safety as it occurs. Training will be passed on to staff.

Data Security

- Any information covered by the Data Protection Act must not be taken out of school on laptops or memory sticks unless encrypted. Information should be backed up and a copy retained in school.

Social Media policy

- Any adults working in, volunteering in or visiting school must adhere to our Social Media policy in addition to staff, parents and other stakeholders.

The Rights of Every Child

Woodthorpe JI School uses the U.N. Convention of the Rights of the Child to ensure that every policy supports the improvement of life chances for children.

Related policies: E. Safety Policy; Policy for 'Use of Images of children', Acceptable Use Policy for Children; Code of Conduct; ICT policy, Data Protection Acts, Behaviour and Anti-bullying Policy, Social Media policy, Child Protection Policy; Safeguarding Policy.

This policy will be reviewed annually.

Signed:

Approved: 25th January 2018

Review: January 2019