Wetherby Senior School

NETWORK USE POLICY

Primary person responsible for this policy: Christine Pheiffer
Job title: Deputy Head Pastoral
Last review date: June 2021
Next review date: June 2022
Relevant ISI coding (if applicable):

Circulation: This policy has been adopted by the governors and is available to parents on request. It is addressed to all members of staff and volunteers and applies wherever they are working with pupils.

'Parents' refers to parents, guardians and carers.

Expectations of pupils

All pupils are encouraged to use ICT resources to support their programmes of learning. Pupils have no right to use ICT resources for other purposes (e.g. personal recreational, administrative, or commercial) which are not connected to their programme of learning.

Pupils are expected to:

- **At all times when in School, devices must be logged on to the School's wifi network and at no times must mobile devices be connected to mobile data accounts for use in School**
- ask questions and share any concerns or confusion they have about how to interact with ICT
- demonstrate a responsible approach to ICT usage, show consideration for all other users, and treat ICT resources with care and respect
- be clear, polite, respectful and responsible in all electronic communications and use of social media, remembering that they must not write, nor post on-line, anything which could embarrass themselves, other pupils, staff, parents or the School if it later became more widely seen than was originally intended
- obtain permission from a staff member before connecting any personal electronic device with the ICT resources of the School; removable storage (memory sticks, external hard drives, CDs/DVDs) must be virus-checked before being connected to the School ICT resources
- observe all the conditions of usage laid out in this policy, **avoid the prohibited content and activities as listed**, and follow the direction of staff members supervising any area where networked resources can be accessed
- report immediately to a staff member wherever they encounter breaches in the controls and security of the network, or where they observe any abuse of ICT resources
- sign, and/or have a parent/guardian sign on their behalf, the acknowledgment in Appendix 1 which confirms that they have read, understood and agree to comply with the ICT Usage Policy

Any pupil who knowingly abuses the privileges of ICT resources will face disciplinary procedures.

Expectations of Staff and Parents

The prohibitions listed will have little significance and effect in practice without an ongoing commitment by staff and parents to:

a) promote understanding amongst pupils of why things are prohibited
b) stay vigilant to the actual behaviour of pupils in their interaction with ICT
c) establish an environment where pupils are encouraged to talk and ask questions about their interaction with ICT, and where they can feel safe sharing their concerns
d) talk to each other (parents and staff) to share information and concerns

Controls, privacy and reporting of breaches

Log-on details (account names and passwords) for access to ICT resources must be kept secret and must not be written down or shared. All users must remember to log-off when they are not in close physical proximity to the machine or device to which they are logged-on. Computers and other user-controlled ICT resources should be either switched off or put on 'stand-by' after use, and especially at the end of the day.

In accordance with statutory guidance, and with the aim of mitigating the risk of harmful behaviour and access to harmful materials, the School ICT resources are subject to various preventative and detective controls such as anti-virus protection, internet- and email-filtering, and usage-monitoring. Consequently pupils should not expect their usage of School ICT resource (including email and internet browsing), nor any of the material they store using School ICT resources, to be private or confidential. The School has the right to search and delete any material where it has grounds to suspect that such material may be harmful to the welfare of pupils.

Staff must remain alert to actual and potential breaches of security and of prohibited content and activities. Pupils are encouraged to look after each other, and to tell staff if they become aware of prohibited content or activities, or weaknesses in network security or internet filtering. Staff must report actual or potential breaches or weaknesses to wssitsupport@wetherbysenior.co.uk, in addition to any other reporting processes as required by other policies (Safeguarding, Anti-Bullying, E-Safety), for example to the Designated Safeguarding lead (DSL).

List of prohibited content and activities

The ICT resources of the School or personal lap tops, phones or any other mobile devices must not be used to search for, create, store, receive or transmit any materials, nor to engage in any activities, which are either illegal or prohibited by this policy. This is a long, but non-exhaustive list. Whilst the School endeavours to educate pupils about all the items on this list, pupils (and parents) should ask for help where they are not clear about any of the issues listed.

(a) Prohibited content and materials are those which are or may be deemed to be:

- racist, sexist or causing any form of prejudicial offence
- threatening, abusive or inciting violence
- obscene, indecent or pornographic
- age-inappropriate[1]
- defamatory[2]
- promoting extremist[3] views
- promoting intolerance of the beliefs, sexuality or life choices of others
- likely to mislead or deceive others
- likely to cause unnecessary stress or anxiety to others

(b) Prohibited activities include:

- bullying (also known in this context as cyber-bullying – see our *Anti-Bullying Policy*)
- harassment – unwanted attention, pestering or persecution (including insults and 'jokes')
- arranging to meet in person with someone first met online (without first checking with parents or teachers)
- writing or posting content on the internet, social media, or school/college network anything which may cause harm or offence to other pupils, parents, staff or to the school/college
- sexting[4]
- 'trolling' – mischievously or maliciously upsetting or offending people on the internet or social media by posting inflammatory remarks
- pretending to be someone else, or theft of someone's identity
- gambling
- promotional, advertising or other commercial activities (unless authorised by staff)

[1] Either explicitly labelled as such (e.g. by censorship, classification, parental guidance) or judged to be age-inappropriate through the application of common-sense.
[2] Defamation is the publication of material which adversely affects the reputation of a person or organisation.
[3] 'Extremism' is defined as vocal or active opposition to *fundamental British values*, including democracy, the rule of law, individual liberty, mutual respect, and tolerance of different faiths and beliefs. Extremism includes calls for the death of members of our armed forces, at home or overseas.
[4] The sharing of sexually explicit images (e.g. naked 'selfies') through mobile phones, the internet or other digital media. In relation to images of people under the age of 18, this is a crime with potentially very serious consequences (Sexual Offences Act 2003)

- plagiarism – i.e. passing-off as one's own work (by copying or closely imitating) the words or creations of others; this includes (for example) copying and pasting content from the internet, **without** clearly acknowledging[5] the original author/creator
- piracy - the unauthorised reproduction or distribution of any 'content' (e.g. books, music, films, videos, games, photographs and images) which are protected by copyright
- hacking (deliberate unauthorised access to websites, devices, networks, systems or databases)
- taking photographs and making audio or video recordings of other people, and distributing such images or recordings, without first obtaining their permission
- unauthorised uploading, such as software licensed to the school/college, or data owned or protected by the school/college or by others
- use of peer-to-peer (P2P) sites or networks unless explicitly authorised by the ICT Coordinator

- activities that might:
  - waste staff effort or network resources
  - corrupt, delete, or destroy other users' data
  - violate the privacy or other rights of other users
  - disrupt the work of, or deny service to, other users

- activities that might affect the proper functioning of ICT resources such as:
  - disabling or overloading any computer system or network,
  - attempting to disable, defeat or circumvent any system intended to protect privacy, security, or intellectual property rights (e.g. copyright)
  - installing or connect any devices, software applications (including games) without authorisation
  - altering system settings, desktop wallpapers, icons etc. without authorisation
  - introduce viruses, worms, Trojan horses, trapdoors or similar programmes
  - interfering with power supply or data cabling

Agreement:

All boys must sign the declaration form. Parents are asked to counter-sign to confirm that they have read this policy.

https://forms.office.com/Pages/ResponsePage.aspx?id=jxr09aJEwkePiM0c9RQhWPv-VmNz6NFHulgW6z75-ShUOTQ0REQzR1AyUExXNDQzSUUwTExKWFZKQS4u

[5] Citing a source (i.e. listing the name of the author, and where and when it was published) is strongly encouraged, not only because it avoids **plagiarism** but, if it is a relatively small extract of the source work, and if done in good faith for educational purposes, it will also significantly reduce or eliminate the risk of any claim for **copyright infringement**.