<u>Acceptable Use Policy</u>

<u>Online Safety - Acceptable Use Statement of Practice</u>

<u>Introduction</u>

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers, they may also arise through the use of games consoles, mobile phones, tablets and other handheld devices.

At Haughton School we ensure that we have in place appropriate policies and statements of practice to promote the safety of our learners; both when they are in the school and when they are elsewhere. We wish to encourage and support the positive use of ICT to develop curriculum and learning opportunities in school. However, as a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. In school we regularly deliver assemblies on keeping safe online, as well through Computing lessons and PSHEE lessons in class.

The school has a duty to keep pupils safe from radicalisation and extremism. Mobile phone use is not permitted for pupils in school. If a pupil brings a mobile phone or tablet to school, they are kept in locked in the school office until the end of the day. Pupils do not have access to their personal device during school hours. Regular online safety advice and updates is shared with parents through the Wake Up Wednesday weekly releases (<u>https://nationalonlinesafety.com/faqs/wakeupwednesday</u>). The school also, ensures filters are set so if devices are sent home, school internet search filters are maintained at home. Therefore, any device taken home by a member of staff or pupil will not have access to inappropriate searches which may include sexual content, social network access, radicalisation, terrorism and extremism.

All staff have annual online safety training and any staff who have concerns are aware of their duty to refer to the designated Safeguarding lead or Online Safety Coordinator.

<u>Aims</u>

This policy is designed to ensure that members of staff are fully aware of their professional responsibilities when using any form of ICT.

<u>Online Safety Rules for Foundation Stage</u>

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.

- I will only use the program or website that my class is working on.

<u>Online Safety Rules for KS1</u>

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.

- I will only use the program or website that my class is working on.

- I will treat other children's work with respect.

- I will tell an adult if I see anything online that I am uncomfortable with.

- I will remember to follow the online safety rules at home.

<u>Online Safety Rules for KS2</u>

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.

- I will not go on inappropriate sites. If I do this accidentally, I will tell my teacher.

- I will tell an adult if I see anything that I am uncomfortable with online.

- I will make sure I am respectful when writing online and will always use positive comments.

- I will make sure I do not copy anyone else's work or information from the internet and pretend it's my own.

- I will remember to follow the online safety rules at home.

- I will only use the names and pictures of my friends if they say it's OK.

- I will only send emails or messages to teachers or to discuss schoolwork.

- Out of school, I know I must not arrange to meet anyone that I don't know.

<u>Acceptable Use Policy for school staff</u>

Any messages, photos, videos or other media I post online will be out of my control. Any inappropriate searches on the internet will be reported to school.

I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to: o pornography (including child pornography)

  - promoting discrimination of any kind to promoting racial or religious hatred
  - promoting extremism and radicalisation o promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling

- do anything which exposes children in my care to danger of any other information which may be offensive to colleagues.

• Forward chain letters, breach copyright law, do anything which exposes children to danger including, take images of pupils out of the premises on removable media or taking sensitive pupil information off the premises on removable media that is not encrypted When using ICT equipment,

I will not:

• Give anyone access to my login name or password

• Attempt to introduce any unlicensed applications

• Corrupt, interfere with or destroy any other user's information

• Release any personal details of any colleague or pupil over the Internet

• Use the school internet access for business, profit, advertising or political purposes

• Leave my account open at the end of a session – remember to 'lock' the screen.

When using email I will:

• Only communicate with pupils, parents/carers and other professionals via a school provided email address or telephone number.

• Observe 'network etiquette' on all occasions. Email or messaging should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny.

• Make sure that nothing in messages could be interpreted as libellous

• Not send any message which is likely to cause annoyance, inconvenience or needless anxiety

When working on professional documents that contain school-related information I will:

• Ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018.

• Not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones or memory sticks), unless they are secured and encrypted.

• Protect the devices in my care from unapproved access or theft

• Not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

When using outside systems, I will:

• Make sure that any information I share on social networking sites takes into account my role as a member of staff

• Not allow pupils to be "friends" with me on social networking sites.

- Keep data about students safe and be responsible for ensuring that the data protection act is not breached.

This policy applies to both fixed and mobile internet; technologies that are in school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by staff that are brought onto school premises (such as laptops, mobile phones, memory sticks etc). The school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes, but occasional personal use is permitted. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

<u>ICT Acceptable Use Policy Agreement for Staff</u>

• I have read, understood and accept the ICT Acceptable Use Policy. I agree that all members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.

• I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

• I also understand that if I am found to have contravened any of these requirements that I may face disciplinary action.

• I accept that my use of the school IT facilities are monitored and the outcomes of the monitoring may be used.

Name:

Signed:

Date: