Online Safety Policy (Staying Safe Online)

Date: November 2022 **Review Date: November 2023**

Introduction

At Springhead School we take Internet Safety very seriously and see it as our duty to keep our pupils safe whilst using technology not only in school but also at home, by informing them and their families of safe internet practice. This also includes our responsibility to keep our children safe from radicalisation and extremism (Prevent Duty).

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

The policy covers 3 main areas; children's safety, staff's responsibilities and support for parents. Our school is a member of National Online Safety (NOS).

E-Safety responsibilities

The Online Safety policy is written and reviewed by the Senior Leadership team and ratified by the school's Governing Body. The policy will be reviewed if any new guidance regarding children's online safety is published by the Government.

Network Safety

The school's Network is presently overseen by NYCC Schools ICT, the School Business Manager, and the ICT co-ordinator, with any issues raised with our school technician. A weekly meeting takes place between the technician and the ICT Co-ordinator. During this meeting any issues with the Network and E-Safety issues are dealt with.

The school network is managed by Smoothwall which is updated and monitored by Schools ICT to make sure it is protecting our staff and students from all forms of inappropriate material.

Training

Springhead School subscribes to National Online Safety (NOS), which provides comprehensive training through courses, webinars and user friendly guides and is available to all staff, students, governors and families. Staff and Governors complete annual training in "Online Safety" in line with the latest Prevent and KCSiE documents, as well as "Maintaining your Online Reputation" which reinforces what is expected of them as professionals.

Safety and Responsibilities for Staff

All staff are required to read "Online Safety Guidance for Schools and in North Yorkshire" and sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the work place. This will be signed when they commence their employment at Springhead School and will be re-enforced each year following E-Safety training.

All staff will complete annual training on E-Safety (through NOS), Prevent - dealing with radicalisation & extremism (NYCC) and Child Protection (UK Gov.)

The AUP list the responsibilities of all staff and covers the use of digital technologies in school: i.e. **E-mail, Internet, Intranet and network resources,** Learning Platform, software, **equipment and systems and complements the** General Teaching Council's Code of Practice for Registered Teachers**.**

All staff will agree to the Code of Conduct (See Appendix 1)

E-Safety and Prevent training will be provided to all members of staff at least once a year and it is each person's responsibility to attend this session. These sessions will be arranged by the ICT coordinator.

It is essential that staff make sure that pupils they are responsible for are using the Internet safely. High risk students will be highlighted and monitored.

Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance. This will include (but is not limited to:

- the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the setting
- Members of staff are encouraged not to identify themselves as employees of Springhead School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role

Communicating with students and parents and carers

- All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the headteacher
- Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher/manager
- Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputies).

Official Use of Social Media

Springhead School official social media channels: Twitter @SpringheadSpSch and Facebook @springheadschool

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the Senior Leadership Team.

Members of the Leadership Team have access to account information and login details for our social media channels. All activity on social media is closely monitored by ICT co-ordinator.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only

- Official social media sites are suitably protected and linked to our website.
- Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: antibullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used
- Any official social media activity involving students will be moderated if possible
- Parents and carers will be informed of any official social media use with students; written parental consent will be obtained, as required
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels

Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Always be professional and aware they are an ambassador for the setting
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so
- Not engage with any direct or private messaging with current, or past, students, parents and carers.
- Inform their line manager, the DSL (or deputies) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from students.

Safety and Responsibility for Pupils

We have a number of pupils who are able to use the Internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

No child is able to access the Internet in school without their parents giving permission to do so. This consent form is filled in at the beginning of each school year. All children are supervised in school whilst using the Internet and all are made aware that all their activity within school is monitored.

All pupils who are able will have to sign an AUP and this will be completed every year during the students E- Safety session. This document will clearly state their responsibilities when using technology in school.

All pupils will receive E-Safety training at the beginning of each term, either as part of their ICT session or PHSE session. (E-Safety materials including lessons plans, PowerPoints and videos can be accessed through NOS.) We will also seek the opportunity to hold sessions throughout the year provided by outside agencies. These extra sessions

would also cover the issue of sexting which could be a serious issue for some of our students due to their learning difficulties.

All pupils will be taught how to use all technologies in a responsible and safe way. This will be part of the ICT curriculum.

No child may appear on the Web Site or social media platforms without their parent/carers consent. The consent form is completed at the beginning of each academic year.

(See Appendix 2 for Acceptable Use for Pupils)

Support for Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

All families are able to access NOS and complete courses and training, as well as seeking specific help. There is also information available to assist with setting up parental controls and promoting the safe use of ICT. Parents are informed of this through letters home and social media posts.

Links

North Yorkshire County Council Online Safety Guidance for Schools

Revised Prevent Duty document (HM Government, July 2015)

Staff Recruitment and Induction

Volunteers in School

Code of Conduct

Behaviour and Discipline Policy

Keeping Children Safe in Education 2022

Health and Safety Policy

Managing Allegations Against Staff

PSHE Policy

Relationships, Sex Education Policy

Staff Handbook

Child Protection and Safeguarding Policy

Appendix 1

Springhead School

Acceptable Internet Use Agreement – Staff/ Governors/ Volunteers

I understand that I must use, promote and model the school's positive use of ICT systems, new technologies and e-safety in a responsible way and for professional purposes to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I am aware that it is a criminal offence to use any ICT system other than those permitted. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students. All users have an entitlement to safe Internet access at all times.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications. I will only access information on schools' servers through a controlled mechanism, with access granted on a need-to-know bases/least privilege basis. I will be vigilant within accessing sensitive or personal information to ensure that no one else, who may be unauthorised, may see the information.
- I will only use school ICT equipment / mobile phones for school purposes and not for personal or recreational use. I will not use any personal devices for any school business unless accessing a secure online platform specifically provided by the school. I will not access any personal accounts (including emails) on school equipment.
- I will not store any school data (in line with the school's Data Protection Policy) on personal devices.
- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes, including hardware and software (apart from a printer at home) of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies and without permission from the ICT/Network Manager.
- I will not access, disable or cause any damage to school equipment, or the equipment belonging to others or access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology.
- I will not browse, upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others or considered offensive. I will report any accidental access of inappropriate materials to my line manager. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. If I need to access what might be considered inappropriate materials – for legitimate research purposes – then I will gain permission in advance from the school's Headteacher. Any such access must not be made when students are present.
- I will respect and comply with copyright and intellectual property rights.

Passwords and Security

- I will not disclose any of my username and password to anyone else, nor will I try to use any other person's username and password. I will protect my passwords and email, network, CPOMS, SharePoint and other school system login information, and should lock (Ctrl-Alt-Del) or log off the network and other systems when leaving a workstation or electronic device unattended. Personal passwords should be entered each time I log on: passwords should never be remembered in automated log on procedures. The ICT technician should be contacted immediately if a member of staff suspects that their password has been compromised.
- I will password protect any portable device that is used to access e-mails or to collect assessment information. These devices should not be used by pupils.
- I will not open any attachments to emails or click on links, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand that data protection policy requires that any staff, governor or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will only transport and hold data about others that is protected by the Data Protection Act and GDPR 2018 in an encrypted manner. I will not transfer any data to any personal devices. I will ensure that all personal data of pupils/staff/parents is kept private and secure and is not held longer than outlined in the schools Document Retention Policy and in accordance with the General Data Protection Regulations 2018. Any data which is being removed from the school site should be encrypted using school approved methods. For this purpose staff laptops are configured with the same security levels on and off site. Personal data sent over the internet should use the NYCC approved systems.

In my professional communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. I will not contact, communicate with or befriend pupils, parents or conduct school business using personal email addresses, telephones, social media without specific permission from the school's Headteacher and will not share own personal details such as telephone/mobile number and address.
- I am aware that emails can be part of Freedom of Information requests so all my correspondence will be professional, courtesy and respectful
- I will not engage in any on-line activity that may compromise my professional responsibilities. I will ensure my use of web-based technologies, including social networking sites, such as Facebook, Twitter etc and chat facilities, does not question or bring their professional role into disrepute and are used in accordance with the school's policies. I am aware that once posted online, by me or others, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- I am aware (and comply) with the Social Media Policy (part of Online Safety Policy)
- I will only communicate with student and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not 'discuss' any school issues on social media.
- I will ensure that all electronic communication with pupils and staff is compatible with their professional role. E-mails sent to an external organisation should be written carefully, and reviewed, before sending, in the same way as a letter on school headed paper.

Photos and videos

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. **No photos of pupils will be taken on any mobile phones**. I will only take and use digital photographs and videos for legitimate reasons. Images of pupils must only be used within school electronic systems (Sharepoint, Evidence for Learning) and must not be made public, e.g. by posting on the internet, without permission of the school's Headteacher and express permission of the parents. Current consent status for the use of pupil photographs is viewable within SharePoint.
- Must not make video or audio recordings (e.g. recording a teaching session), or take digital images of other members of staff without the express, prior permission of those staff.

Reporting

- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person
- I will report any suspected damage to the ICT system due to virus or malware to immediately as well as any suspected damage to a school system.
- I will report all incidents of concern regarding children's safety on line to the Designated Safeguarding Lead (DSL) immediately
- I will immediately report any damage or faults involving equipment or software, however this may have happened. Theft of any school devices must be reported to the ICT/Network Manager immediately.

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I have read and understand the above and agree to comply and use the school ICT systems (both in and out of school) within these guidelines. I understand that I am responsible for my actions in and out of the school and if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and, in the event of illegal activities, the involvement of the police. If I need more support, I know I can access information about e-safety on Sharepoint and National Online Safety.

- Print Name ……. Signed …… Date ……

Appendix 2

Springhead School

Acceptable Internet Use Policy – Pupils

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems / devices for personal or recreational use, for accessing social media sites, on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/ipod) in school at times that are permitted. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line.
- I will not take, or distribute, images of anyone else without their permission.
- I will not take, or distribute, images of myself or anyone else semi-naked or naked.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Pupil Signed ……..

Date …….

Parent / Carer Signed ……..

Print Name…….

Date……..