ONLINE SAFETY POLICY

1. Rationale. The use of 'Information and Communication Technologies (ICT)' has great benefits for the development of students' learning and the administration and governance of a school. With these advantages, however, come significant risks, including: sexual exploitation, identity theft, spam, 'cyber' bullying, viruses.

It is the aim of this policy to minimise these risks for students, staff and others involved with the daily activities of the school.

This policy supported by the school's Acceptable Use Agreements for staff and students is to protect the interests and safety of the whole school community. It is linked to the following school policies:

a. Anti-Bullying
b. Behaviour
c. Child Protection including Prevent strategy (Safeguarding)
d. Sex and Relationship Education
e. Mobile Devices

2. What is 'Un-Safe' Use of ICT? This policy is concerned with significantly unsafe use of ICT, not minor infringements. Just as safe use of ICT is commonly known as e-safety, unsafe use of ICT is an e-safety incident. E-safety incident:

- uses some form of technology
- leads or could lead to the commission of a criminal offence or causes or could have caused harm or distress to others either within or outside the school
- may or may not be deliberate
- may not have occurred within school or on school equipment

Examples of e-safety incidents (not exclusive) include:

- a student or member of staff viewing pornography on a school computer
- a student bullying a fellow student with text messages or by using instant messaging services such as MSN, Instagram or Snapchat from home
- a student placing distressing posts about a member of the school community on social networking sites like Facebook
- a student publishing their own address details on the internet
- a student publishing revealing images of her or himself on a social networking site
- a student sharing a phone video of a member of staff in a lesson with other students
- a member of staff suspecting a student of being groomed by a paedophile through their use of internet chat services
- a student modifying a photo of a member of staff and distributing it leading to offence
- a student or member of staff trying to hack into or attempting to gain access to any computer system for which authorisation has not been expressly given.
- a student or member of staff engaging in any criminal conduct or any conduct that could be said to promote or encourage the commission of any criminal offence, including the encouragement of terrorism and/or the dissemination of terrorist images and publications.

3. Staff Responsibilities

Roles and Responsibilities of the Headteacher

- Supporting the Governors to comply with the online safety aspects in the current edition of Keeping Children Safe in Education.
- The safety (including online safety) of all members of the school community.
- Ensure effective and regular training about online safety is provided for the whole school community and a log is kept of the staff who complete the training
- Invite governors to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety education, health and safety or child protection.
- Ensure effective communication with parents/ carers about safe practices when using online technology's and support them in talking to their children about these issues
- Ensure effective filtering, monitoring and security systems are set up
- Ensure there are effective procedures in place in the event of an online safety allegation which are known and understood by all members of staff
- Establish and review the school online safety policy and documents and making them available on the school website
- Ensure the school's Designated Safeguarding Lead is trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.

Roles & Responsibilities of a named member of the Senior Leadership Team who may also be the Headteacher:

- Liaising with staff, ICT Technical staff, online safety governor, SLT and partner agencies on all issues related to online safety
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff and keeping a log of staff who complete training about online issues
- Keep a log of staff, students and families who have signed the Acceptable Use Policy (AUP) for the safe use of technology
- Receive and respond to reports of online safety incidents and creates a log of incidents and outcomes to inform future online safety developments
- Co-ordinating and reviewing online safety education programme in school, working in partnership with the Pastoral team and the Teacher in Charge of ICT.

Roles & Responsibilities of the Network Manager (supported by the Bursar):

- The school's ICT infrastructure is secure and meets requirements for filtering and monitoring
- The school's website is kept secure from 'hacking' and there is an action plan in place if it is hacked
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Keeps up to date with online safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the named SLT for action.

Roles & Responsibilities of all staff:

In addition to the elements covered in the Staff Acceptable Use Policy (Appendix 2), all staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the schools current online safety policy and practices
- They attend the training provided by the school about online safety and all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy, Acceptable Usage and Child Protection Policies.
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- They do not 'befriend' any student or student family member on social media in a social context whilst the student is at the school

- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's online safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courtesy and respectful
- If confidential information / information under the data protection act is being sent by email it must be sent through the secure email system which if provided by Schools ICT would be the Egress system which the schools administration and headteacher have access to but more licenses can be purchased.

4. Roles & Responsibilities of all students:

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy also covers their actions out of school, if related to their membership of the school or using equipment provided by the school.

5. Roles & Responsibilities of all parents/carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Schools will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Usage Policy and will, alongside this, sign to say they support this policy.
- Ensuring that they do not use social media to criticise or make inappropriate comments about the school or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If a parent/ carer has any concerns about anything which happens in school, they should contact the school directly.

Parents and Carers should also be aware of the health effects of children and young people having too much 'screen time'. This can limit the amount of time children are being physically active, reduce the amount of time they are sleeping and could be impacting on their eyesight. A number of systems and apps are available that can limit the screen time for children and young people alongside parents and carers talking to their children about the issues. The school website provides information for parents/carers to access to support them in protecting their children and ensuring they stay safe online.

NSPCC online safety https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/	Provides helpful advice and tools that a parent/carer can use to help keep their child safe whenever and wherever they go online. • Has material and information for use with young children as well as older children • Key advice for parents / carers • Information on a range of social media sites and games
Thinkuknow https://www.thinkuknow.co.uk/parents/	Provides helpful advice and tools that a parent/carer can use to help keep their child safe online. They have downloadable guides for parents/ carers on various social media sites like Instagram, Whatsapp, youtube etc They also have some useful films for parents to watch about the risks online and four specific films about sexting / 'self nudies' and how to talk to their children about this issue and what to do if this happens.
Childnet http://www.childnet.com/parents-and-carers The whole website can be read in a variety of languages.	A range of information to support parents/ carers keep their children on safe including: • Parents: Supporting Young People Online (Leaflets in a variety of languages) • Key advice for parents / carers • Conversation starters to enable parents /carers to talk to their children • How to set parental controls on a range of devices • Gaming
Safer internet http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers	Very specific advice, films and signposting to ensure parents/ carers have the information about how to set up parental controls on a range of devices and their home internet
North Yorkshire Local Children Safeguarding Board (LCSB) http://www.safeguardingchildren.co.uk/parents-and-carers	In partnership with other agencies the LSCB have developed an information leaflet containing practical advice about how parents/ carers can support their children stay safe online

6. Staff training Opportunities. It is important that staff are kept up to date with online safety issues for children and young people but also for them to consider their online presence.

North Yorkshire County Council provide training opportunities for staff through the Education and Skills team. The Headteacher ensures that staff, in particular the Designated Safeguarding Lead, Deputy Designated Safeguarding Lead, and other members of the Pastoral Team, have access to relevant training and courses. A record of the training and courses attended by staff is logged through the safeguarding audit and reported to governors during the annual safeguarding report. Annual staff training will incorporate the staff use of ICT for themselves and for the students they supervise. This will include the Keeping Children Safe in Education training delivered in conjunction with NYCC guidance. All new staff and volunteers will meet with the DSL as part of their induction and the Online Safety Policy will be explained.

All staff training will raise awareness of their individual responsibilities for the Safeguarding of children within the context of online safety and cover what to do in the event of misuse of technology by any member of the school community.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

7. Online Safety Education for Students will be provided in the following ways:

- A planned online safety programme is provided as part of the PSHE and assembly programme and is regularly revisited in Computing and other lessons across the curriculum. This programme covers both the use of ICT and new technologies in school and outside of school.
- A range of safeguarding issues are considered as part of the online safety education: keeping their personal information private, healthy relationships on and offline, grooming, sending inappropriate images and the consequences of this, gaming, gambling, radicalisation and how to recognise the signs and keep themselves safe
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

For information and clarification of the use of mobile devices including mobile phones in school, please refer to the school's Mobile Devices Policy.

8. Managing the use of Technology

Infrastucture. Nidderdale High School will monitor access and use of the school network including internet services, so activity is monitored and recorded. Email and internet activity can be monitored and explored further if required. Nidderdale High School will be aware of its responsibility when monitoring staff and student communication under current legislation and take into account:

- Data Protection Act 2018
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998

The school will use management control tools for controlling and monitoring workstations.

Appropriate use of Email

Digital communications with students and parents / carers (e-mail, online chat, VLE, voice etc.) will be on a professional level and only carried out using official school systems

- The school's e-mail service should be accessed via the provided web-based interface by default
- For all school purposes, students and staff will use their school email accounts. Under no circumstances will staff contact students, parents/carers or conduct any school business using personal e-mail addresses
- School e-mail is not to be used for personal use
- All staff are aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courtesy and respectful
- If it is necessary to email confidential information / personal information, it must be sent (ensuring that data protection principles are adhered to) through the secure email system provided by Schools ICT (Egress)

Appropriate use of mobile phones (See also Mobile Devices Policy)

- School mobile phones will only be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices and under no circumstances should a student or parent/carers be given the personal mobile number of a member of staff

- Staff should not be using personal mobile phones in school during working hours when in contact with children
- Visitors will be asked not to use their mobile phone whilst on site with any students present due to all mobile phones containing a camera
- Students should adhere to the rules and guidelines set out in the Behaviour Policy / Mobile Devices Policy regarding mobile phone use in school
- All students will be required to put their phone / interactive watch in a secure container at the start of any PE lesson before students start to get changed
- All students will be required to hand in their phones / interactive watches which will be placed in a which will be placed in reception for the duration of the exam

Appropriate use of social networking sites

- Staff will not access social networking sites on school equipment in school or at home that have not been pre-approved by the school
- Staff users will not refer to any member of staff, students, parents/carers, the school or any other member of the school community on any social networking site or blog in a derogatory way
- Students will not be allowed on social networking sites on school equipment that have not been pre-approved whether in school or at home. At home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites
- Students/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or members of the school community
- Parents / carers and students will be informed that they do not use social media to criticise or make inappropriate comments about the school, an individual member of staff or another student as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/ carer they have any concerns about anything which happens in schools then they are asked to contact the school directly
- If inappropriate comments are placed on social networking sites about the school or school staff then advice will be sought from the relevant agencies, including the police if necessary
- Students will be taught about online safety when using social networking sites

Appropriate use of digital images

- The school record of parental permissions granted/not granted will be adhered to when taking images of our students.
- Under no circumstances should images be taken by staff or Governors using privately owned equipment
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file
- Visitors / contractors will be asked not to use their mobile phone whilst on site with any students present due to all mobile phones containing a camera
- Parents/carers are requested not to share images from a school event if they include children other than their own

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. For example, the school uses its website and Twitter to inform/publicise school events and celebrate and share the achievement of students. The website includes copies of the Nidd News, Newsletter publications and links to Newspaper articles.

Removable Data Storage Devices

- Only school provided removable media should be used and they should be encrypted
- Any information that is on removable data storage device for school use should not be transferred onto any personal devices, in particular any information that is covered by the data protection act and could lead to an individual being identified
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks

- Students must not bring their own removable data storage devices into school for use on school equipment.

Appropriate use of websites

- In lessons where Internet use is pre-planned, students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches
- Staff will preview any recommended sites before use
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with students who may misinterpret information
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents are advised to supervise any further research
- All users must observe copyright of materials published on the Internet
- Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is monitored and logged.
- The school only allows the Network Manager and SLT to access Internet logs.

Use of passwords for students

- Students should only let school staff know their in-school passwords
- Students should not share their password with another student / sibling
- Students should inform staff immediately if passwords are traced or forgotten. Some staff are able to access the network to allow students to change passwords

Use of School ICT Equipment

- Privately owned ICT equipment should never be connected to the school's network and no personally owned applications or software packages should be installed on to school ICT equipment
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted
- Staff will ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access

Monitoring

All use of the school's Internet access is logged, and the logs are randomly but regularly monitored by the school's external provider. Schools access Smoothwall's reporting mechanism which will identify students that are searching for websites / using search words that may be inappropriate. It will also highlight issues through the content of the site e.g. reference to suicide.

9. Responding to incidents of misuse

Any online safety incidents must immediately be reported to the designated safeguarding lead or deputy designated safeguarding lead if it is a member of staff, student or parent/carer who will investigate further following online safety and safeguarding policies and guidance.

It is hoped that all members of the school community will be responsible users of ICT. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the school may involve the Police. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as

possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

10. Sexting in Schools

For the first-time, there is clear guidance to schools about how they should handle incidents where students under-18 take and/or share naked images of other under-18s, including themselves. This new guidance takes a safeguarding focus, rather than a simple criminal response, and, in some circumstances, allows schools to deal with incidents without involving the police.

There is no clear definition of 'sexting'. Instead, this document talks about 'youth-produced sexual imagery'. This is imagery that is being created by under 18s themselves and involves still photographs, video, and streaming. In the guidance, this content is described as sexual and not indecent.

Incidents covered by this guidance:

- Person under 18 creates a sexual image of themselves and shares it with another person under 18.
- A person under 18s shares an image of another under 18 with another person under 18 or an adult.
- A person under 18 is in possession of sexual imagery created by another person under 18.

Incidents not covered by this guidance:

- Under 18s sharing adult pornography.
- Under 18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under 18s. (This is child sexual abuse and must always be reported to police.)

Date reapproved by Governing Body – 29 June 2020
Next Review June 2023

Appendix 1

Acceptable Internet Use Policy – Students

This document is both a code and 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 IT and 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 have read the school's latest edition of its On-Line Safety Policy
- 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 on any computer system.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal handheld 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 unnecessarily strong, aggressive or inappropriate but 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 can 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 arrange to meet 'on-line friends'.
- 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 I receive 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.

Student Signed ……Date …….

Parents/Carers must also sign this document to state they endorse the Online Safety Policy and will support their child in understanding the need to use the internet/mobile devices in an appropriate way.

By signing this policy, parents/carers are agreeing that they have read the School's Online Safety Policy (see the school website (policies are listed alphabetically under Governance)).

Parent / Carer Signed …… Date……

Acceptable Internet Use Policy – adults who work in the school community (and governors)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All school ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible Use Agreement
I understand and accept that I must use the school's ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. 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.

For my professional and personal safety:

- I understand and accept that the school will monitor my use of ICT systems, email and other digital communications.
- I understand and accept the rules set out in this agreement also apply to the use of the school ICT
- systems (e.g. laptops, email, Learning Platform etc.) out of the school.
- I will only use school ICT equipment / mobile phones for school purposes I will not use any personal devices for any school business
- I understand that the school ICT systems are intended for educational use and that I will not use systems for personal or recreational use.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person

I will be professional in my 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 am aware that emails can be part of Freedom of Information and Data Protection requests so all my correspondence will be professional, courtesy and respectful

- 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.
- I will not use chat and social networking sites in the school in accordance with the school's policies.
- 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 engage in any on-line activity that may compromise my professional responsibilities.
- I will not befriend any present student or their family members on social media
- I will not 'discuss' any school issues on social media
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or terrorist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- 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 of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this has been expressly allowed by the appropriate person or authority or is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport and hold data about others that is protected by the Data Protection Act in an encrypted manner. I will not transfer any data to any personal devices.
- I understand that data protection policy requires that any staff 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 immediately report any damage or faults involving equipment or software, however this may have happened.

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).

Staff using work devices outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
- Work devices must be used solely for work activities.

I understand that I am responsible for my actions in and out of the school:
- 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 the school.
- I understand that 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.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff/Volunteer/ Governor

Name ……..

Signed ……

Date ……

APPENDIX 3

PROTOCOL FOR LIVE AND RECORDED MICROSOFT TEAMS LESSONS

1. All 'live' online interaction with students will have been pre-approved by a member of SLT.
2. All staff will follow the school's agreed protocol for live and recorded online content, this includes not having 1:1 meetings with students online.
3. Lessons will be recorded to enable students to access them at a later date.
4. All members of our school community will follow the expectations of Ready, Respectful and Safe. If any student is unable to follow these expectations, they will be removed from the 'virtual classroom'.
5. Ready, Respectful and Safe: Students must wear clothing appropriate for a meeting with a teacher i.e. not pyjamas or clothing that is revealing.
6. Respectful: students' language and behaviour should always be respectful and appropriate.
7. Respectful and Safe: students should be aware of what is in the background of their video, to protect the privacy of others.
8. Respectful and Safe: Whilst other family members may be present in the room, they should not appear in view of the screen or contribute to discussion.
9. Respectful: Messages to the teacher will be through the typed 'chat' function, students will be invited to unmute their microphone if a conversation is needed.
10. Live classes will be recorded and backed up.

SAFEGUARDING PROTOCOL – INFORMATION FOR STUDENTS

This page explains how to keep safe when using Teams. READ THIS PAGE BEFORE JOINING THE MEETING

1. Invites. Invites will be sent to students, but you must make sure that parents and carers know about and agree to the meetings.
2. Check your background. Check to make sure that nothing private is visible behind you. If available on your device, use the background effects to blur or hide everything except you.
3. Camera off. Only use video if you need to. You do not have to turn on the camera, just listen and chat and not be seen, if you would prefer.
4. Appropriate clothing. All participants should be fully dressed in appropriate clothing, for example no night wear and wearing something that is smart.
5. Parent/carer supervision. A parent or carer should say hello or give us a quick wave at the start at the meeting, so we know an adult is available.
6. Quiet please. Let others in your house know that you are having a Teams meeting, so they don't accidentally interrupt.
7. Settings. Students should only use the settings needed for the purposes of the meeting as set up by the teacher.
8. No recording. No part of the meeting should be recorded, or screenshots taken. If a record of the meeting is needed, then the teacher will do this.
9. Courtesy muting. To assist with sound quality, please mute yourself unless you wish to speak. Unmute yourself to speak then mute yourself again after you have spoken.
10. Talking carefully. To comply with data protection, anyone who is not present should not be talked about, and we must be very careful with the words that we speak.