HORSFORTH SCHOOL

Opportunity and achievement for all

Online Safety Procedures

Last Reviewed	July 2018
Next Review Date	October 2022
Ratified by the Headteacher	October 2019

Online Safety Procedures

1 Aims

The purpose of these procedures is to:

- Safeguard and protect all members of Horsforth School community online.
- Identify what is unsafe use of ICT
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Horsforth School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example fake news, pornography and extremist views
- **Contact:** being subjected to harmful online interaction with other users; for example harmful advertising, CSE
- **Conduct:** personal online behaviours that increase the likelihood of, or causes, harm to others or the individual themselves

2 Context

- We believe that online safety is an essential part of safeguarding and we acknowledge our duty to ensure that all students and staff are protected from potential harm online.
- The school acknowledges that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- We believe that students should be empowered to build resilience and develop strategies to manage and respond to risk online.
- These procedures apply to all staff including the Trustee Board, Members, teachers, associate and support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in these procedures) as well as students and parents/carers.
- These procedures apply to access to the school internet and access to the internet through personal devices. It applies to all students, staff or other individuals who have been provided with school issued devices for use in the classroom or off-site, such as laptops, tablets or mobile phones.
- Whilst care has been taken to consider all aspects of Online Safety there may be times when members of staff, need to make independent judgments on individual situations not covered in this document. It is expected that in these circumstances that all staff will advise their senior colleagues of such. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action. Any student in breach of these guidelines will face appropriate school sanctions.

These procedures have links to and should be read in conjunction with other policies and procedures:

- Anti-bullying Policy
- Positive Behaviour Policy
- Child protection Policy
- Lifeskills (Personal Social and Health Education Policy)
- Mobile Phone Procedures

2.1 "Unsafe" use of ICT:

- Using a form of technology that can invade privacy, cause offence, harm or distress; or put individuals or others at risk
- It may or may not be deliberate
- It may have occurred within school or outside of school
- It may have occurred on school equipment or personal equipment

3 Evaluation

These procedures will be evaluated every three years to ensure it is still fit for purpose. Circumstances may require more frequent modifications. On 8th May 2019, the Trustee Board delegated responsibility to evaluate and ratify these procedures to the Headteacher.

4 Authors

These procedures have been written and developed by the Designated Lead for Safeguarding, the ICT team, E-Learning Manager and the Data Team. It takes into account the DfE statutory guidance "Keeping Children Safe in Education".

5 Appendices

Appendices to support these procedures are attached as follows:

Appendix 1	Roles and Responsibilities
Appendix 2	Education and Training Approaches
Appendix 3	Safer Use of Technology
Appendix 4	Social Media
Appendix 5	Use of Personal Mobile Devices (MPD's)
Appendix 6	Responding to Online Safety Incidents and Concerns
Appendix 7	Procedures for Responding to Specific Online Incidents or Concerns
Appendix 8a	Acceptable Use Agreement– Staff
Appendix 8b	Acceptable Use Agreement for Students
Appendix 9	Useful Links for Educational Settings
Appendix 10	ICT Resources Guidance Document

Appendix 1: Roles and Responsibilities

1a) The leadership and E- Learning team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including an Acceptable Use Agreement, which covers acceptable use of technology for staff and students.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.

1b) The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.

Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.

- Report online safety concerns, as appropriate, to the management team and the Trustee Board.
- Work with the leadership team to review and update Online Safety Procedures on a regular basis (at least annually) with stakeholder input.

1c) It is the responsibility of all members of staff to:

- Read and adhere to the Online Safety Procedures and Acceptable Use Agreement.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online safety concerns and take appropriate action by following the school's Safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

1d) It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate Online Safety Procedures.
- Implement appropriate security measures *(including complex passwords and encryption as and when required)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering procedures are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

1e) It is the responsibility of students

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of Online Safety Procedures.
- Read and adhere to the school -Acceptable Use Agreement.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

1f) It is the responsibility of parents and carers to:

- Read the school Acceptable Use Agreement and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and Acceptable Use Agreement. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school Online Safety procedures.
- Use school systems, such as learning platforms, VLE, app and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Appendix 2: Education and Training Approaches

2a) Education of students

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support pupils to read and understand the acceptable Use Agreement in a way which suits their age and ability by:
    - Displaying acceptable use posters in all ICT rooms with internet access.
    - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology by pupils.
    - Implementing appropriate peer education approaches through assemblies and Tutor time
    - Providing online safety education and training as part of the transition programme across the key stages
    - Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches ie, Police Liaison officer

Vulnerable Pupils

- We are aware that some students are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

2b) Training of staff

The school will:

- Provide the online safety procedure to all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies and procedures when accessing school systems and devices.

- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

2c) Awareness and education of parents and carers

- We recognise that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness evening forums, parent's evenings, email updates and information on the schools web.
    - Drawing their attention to the school online safety procedure and expectations in newsletters, letters and on our website.
    - Requiring them to read the school acceptable Use Agreement and discuss its implications with their children.

Appendix 3: Safer Use of Technology

3a) Classroom Use

- Horsforth School uses a wide range of technology. This includes access to:
  - Computers, laptops, i-pads and other digital devices such as phones
  - Internet which may include search engines and educational websites
  - School learning platform/intranet - VLE
  - Email
  - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's acceptable Use Agreement and with appropriate safety and security measures in place. (Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home).
- The school will use age appropriate search tools to identify which tool best suits the needs of their classes.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

3b) Managing Internet Access

- The school will maintain a record of users who are granted access to the school's devices and systems.
- All staff and students will read and sign the acceptable Use Agreement before being given access to the school computer system, IT resources or internet.

3c) Filtering and Monitoring

- Leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- Leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering procedures are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate through a half termly meeting with online safety team.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.
- The school uses educational broadband connectivity through Schools Broadband.
- The school uses Lightspeed filtering which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list. In addition the Sophos Anti-Virus will attempt to block access to questionable sites e.g. pornographic this service continues to work on school devices even when away from school.

- The school works with our ISP Schools Broadband to help ensure a robust filtering procedure is in place. Schools Broadband is a member of the Internet Watch Foundation (https://www.schoolsbroadband.co.uk/company)

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
  - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff).
  - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead, BST and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: Channel, Police or CEOP.

. 3d) Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

3e) Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on the school's network,
  - The appropriate use of user logins and passwords to access the school network. Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended.

3f) Passwords

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- From year 7, all students are provided with their own unique username and private passwords to access school systems; students are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

3g) Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE) and is reviewed regularly.
- The school will ensure that our website complies with guidelines for publications including: accessibility; GDPR; respect for intellectual property rights; privacy policies and copyright.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

3h) Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated policies and procedures, including (but not limited to): Data security, parental consent, Acceptable Use Agreement and Use of personal devices and mobile phones.

3i) Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies and procedures.
  - Any internal electronic communication which contains sensitive or personal information will only be sent using secure or encrypted email**.**
  - School email addresses and other official contact details will not be used for setting up personal social media accounts

Staff

- Members of the school community will immediately tell the Designated Safeguarding Lead and Director of HR if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

Students

- Students will use school provided email accounts for educational purposes.
- Students will sign an acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

3j) Management of Learning Platforms (the VLE)

- The VLE is the schools official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, students and parents will have access to the LP. When staff and/or students leave the school, their account or rights to specific school areas will be disabled.
- Students and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.

- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement. ie) A students parent/carer may be informed.
    - If the content is considered to be illegal, then the school will respond in line with existing Child Protection and Positive Behaviour and Staff Disciplinary Policies.

3k) Management of Applications which Record Children's Progress

- The school uses SIMS and SISRA to track pupils' progress and share appropriate information with parents and carers.
- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation
- To safeguard data:
    - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content.
    - School devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

Appendix 4: Social Media

4a) Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Horsforth school.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control student and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school hours for personal use is not permitted for students on school site and only for staff during non-contact hours.
    - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of the school community on social media should be reported to the school and will be managed in accordance with our Anti-bullying, Staff Disciplinary Policy, Positive Behaviour and Child Protection policies.

4b) Staff Personal Use of 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 the school Code of conduct within the acceptable Use Agreement.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they 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 and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - 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 school.

- Members of staff are encouraged not to identify themselves as employees of Horsforth School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also 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 with schools 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 pupils 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 in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' 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 Designated Safeguarding Lead and/or the Headteacher.
  - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

4c) Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding students' use of social media, both **at home** and **at school**, will be dealt with in accordance with existing school policies and procedures including Anti-bullying and Positive Behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Students will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples could include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally to school and to CEOP.

Appendix 5: Use of Personal Mobile Devices (MPD's)

- We recognise that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within school.

5a) Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies and procedures, including, but not limited to: Anti-bullying, Positive Behaviour and Child protection policies and Mobile Phone Procedures
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
- All members of the school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used on school site. They must remain in bags at all times, turned off and 'invisible.'
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Positive Behaviour Policy.
- All members of the school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's Positive Behaviour or Child Protection policies.

5b) Staff Use of Personal Devices and Mobile Phones

- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods, break and lunch duty or detention duty or unless written permission has been given by the Headteacher, such as in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school procedures, action will be taken in line with the Staff Disciplinary Policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.
  -

5c) Pupils’ Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- We have a separate Mobile Phone Procedure for students which outline protocols and procedures.

- If a pupil breaches the school rules, the phone or device will be confiscated and will be held in a secure place in the pastoral hub and/or the Deputy Headteacher’s safe.
- School staff may confiscate a pupil’s mobile phone or device if they believe it is being used to contravene the school’s Mobile Phone Procedures, Positive Behaviour or Anti-Bullying policies or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with the school’s policies and procedures.
- Pupils’ mobile phones or devices may be searched by a member of the leadership or a PBO, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies and procedures.
- Mobile phones and devices that have been confiscated will be released to parents or carers in accordance with the School’s policies and procedures.
- If there is suspicion that material on a pupil’s personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Appendix 6: Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must use the official school procedures for reporting concerns through the Cause for Concerns forms and Behaviour procedures.
- The school requires staff, parents, carers and students to work in partnership to resolve online safety issues.
- After any investigations are completed, the CP team will identify lessons learnt and implement any procedure, policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Leeds Duty and Advice Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with to the Police and/or the other school/s.

6a) Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns. The CP officers will record these issues in line with the school's Child Protection Policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

6b) Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher according to the Staff Disciplinary Policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Appendix 7: Procedures for Responding to Specific Online Incidents or Concerns

7a) Youth Produced Sexual Imagery or "Sexting"

- We recognise and identify youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by Child Protection officers and the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

.

7b) Dealing with 'Sexting'

If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:

- Act in accordance with our Child protection and Safeguarding policies
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- Assess the risks to the young person and consider any vulnerability involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to the Police, if appropriate.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support wave 2-3.
- Implement appropriate sanctions in accordance with the school's Positive Behaviour Policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.

The school will not:

- View any images suspected of being youth produced sexual imagery unless there is a clear need or reason to do so. In this case, the image will only be viewed by the Child Protection team and/or Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.

- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

7c) Online Child Sexual Abuse and Exploitation

- We will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for students, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community.

7d) Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
  - Act in accordance with the school's Child protection and Safeguarding policies and immediately notify the Designated Safeguarding Lead.
  - Store any devices involved securely.
  - Immediately inform the police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of students involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Make a referral to Specialist Children's Services (if required/ appropriate).
  - Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support wave 2-3.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Leeds Duty and Advice Safeguarding Team and/or Police.

7e) Indecent Images of Children

- We will ensure that all members of the school community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Police and/or the Leeds Duty and Advice team.

- If made aware of IIOC, the school will:
  - Act in accordance with the school's Child Protection and Safeguarding policies and immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the police or the LADO.

- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school devices, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the Headteacher is informed.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools Staff Disciplinary Policy.
  - Quarantine any devices until police advice has been sought.

7f) Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Horsforth School.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying Policy.

7g) Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing school policies and procedures including Anti-bullying and Positive Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted wherever we suspect hate crime
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the police.

7h) Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection Policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Staff Disciplinary Policy.

Appendix 8a: Acceptable Use Agreement - Staff

This Acceptable Use Agreement is intended to ensure:

- that Horsforth School staff will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that Horsforth School systems and users are protected from accidental or deliberate misuse that could put the security of these systems and users at risk

Agreement:

I understand that I must use Horsforth School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

- I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. (Eg laptops, mobile phones, tablets, digital cameras, email and social media sites)
- Horsforth School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by Horsforth School for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.
- I will respect system security; will not disclose any password or security information, will use a 'strong' password (alpha/numeric/symbol) and change it regularly.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Network Manager.
- I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection legislation, including GDPR.
- I will not keep or access professional documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment.
- I will respect copyright and intellectual property rights.
- I have read and understood Horsforth School Online Safety Procedures which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.
- I will embed online safety education in curriculum delivery wherever possible.
- I will ensure I have an awareness of a range of online safety issues and how they may be experienced by students under my supervision.
- I will identify online safety concerns and take appropriate action by following Horsforth School's safeguarding policies and procedures.
- I will ensure I know how and when to escalate online safety issues, including signposting to appropriate support both internally and externally.
- I will take personal responsibility for professional development in this area.
- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of to the Child Protection Team and/or Headteacher.
- I will not attempt to bypass any filtering and/or security systems put in place by Horsforth School. If I suspect a computer or system has been damaged or affected by a

virus or other malware, or if I have lost any school related documents or files, then I will immediately report this to the IT Support Team.

- My electronic communications with current or past students, parents/carers and other professionals will take place within clear and explicit professional boundaries, and will be transparent and open to scrutiny at all times.
    - All communication will take place via Horsforth School approved communication channels such as Horsforth School email address or telephone number, and not via personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Headteacher.

- I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
- I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, or Horsforth School, into disrepute.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead and/or Headteacher.
- I understand that my use of Horsforth School information systems, including any devices provided by Horsforth School, school internet and school email may be monitored and recorded to ensure the safety of students and staff and to ensure compliance with policies and procedures. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
- I understand that Horsforth School may exercise its right to monitor the use of information systems, including internet access and the interception of emails, in order to compliance with policies and procedures. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, Horsforth School may invoke its disciplinary procedures. If Horsforth School suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Horsforth School Staff Acceptable Use Agreement.

Staff Name: ....

Signed: ....

Date: ....

Appendix 8b: Acceptable Use Agreement - Students

This Acceptable Use Agreement is intended to ensure:

- that Horsforth School students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that Horsforth School systems and users are protected from accidental or deliberate misuse that could put the security of these systems and users at risk

Agreement:

I understand that I must use Horsforth School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that Horsforth School will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password
- I will not disclose or share personal information about myself or others when on-line
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Horsforth School systems and devices are intended for educational use and that I will not use them for personal or recreational use
- I will not use Horsforth School's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube)
- I understand that it may be a criminal offence or breach of Horsforth School policies and procedures to download or share inappropriate pictures, videos or other material online
- I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18

I will act as I expect others to act toward me:

- I will respect others students' work and property and will not access, copy, remove or otherwise alter any other students' files, without their knowledge and permission
- I will be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images of anyone without their permission
- I will not bully anybody online and will not use technology to cause harm or distress.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Horsforth School:

- I will only use my own personal devices (mobile phone/tablet/laptop etc) in school if I have permission. I understand that, if I do use my own devices in Horsforth School I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place at Horsforth School to prevent access to such materials

- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person or organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings
- I will only use social media sites with permission and at the times that are allowed

I understand that I am responsible for my actions, both in and out of school:

- I understand that Horsforth School also has the right to take action against me if I am involved in incidents of inappropriate online behaviour, and this extends to when I am out of school
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, school sanctions and, in the event of illegal activities, involvement of the police.

I, (with my parents/carers) have read and understand that use of Horsforth School IT systems and devices is governed by the Online Safety Procedures and all of the policies and procedures available from Horsforth School's website www.horsforthschool.org when:

- I use Horsforth School systems and devices (both in and out of school)
- I use my own devices in Horsforth School, when permitted (eg mobile phones, tablets, laptops, cameras)
- I use my own equipment out of Horsforth School in a way that is related to me being a member of Horsforth School (e.g. communicating with other members of the school, accessing school email, VLE, website).

Name of Student: ....

Form: ....

Signed: ....

Date: ....

Parent/Carer Countersignature

Parents/Carers should sign below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Name of Parent: ....

Signed: ....

Date: ....

Appendix 9: Useful Links for Educational Settings

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafetyChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Appendix 10: ICT Resources Guidance Document

Horsforth School will provide ICT resources (equipment, service accounts and means of communication) for the purpose of helping you perform your duties, it is expected that this is what they will be used for.
ICT equipment (e.g. PC's, laptops and iPads) are sophisticated pieces of equipment which can be easily damaged by incorrect handling or operation. If this happens it will directly affect your ability to do your job, it is in your best interests to read and understand the guidelines presented in this document.

1. Device Security.

You are responsible for ensuring that when you do not have direct control (can see it) over ICT equipment you have been issued, that it is:

1.1 Kept in a locked classroom/office or in a lockable storage cupboard. Your ICT equipment is insured whilst away from school (an insurance excess of £150 will be billed to your department) provided you have taken due care (e.g. not left it in an unlocked room on open display).

1.2 Unauthorised access is controlled:

1.2.1 For Windows PCs/Laptops (if you are logged in) ensure that it is locked when you are away from the machine by holding down the Windows key ⊞ and pressing **L** .

1.2.2 For tablets devices ensure that a passcode has been setup which only you and IT Services know.

1.3 You must not share or give your device to anyone else, this includes friends and family. Any activity carried out on the device will be your responsibility as if you had undertaken it yourself.

1.4 You must **never share** or give anyone else your password(s) as you may be held jointly responsible for their misuse. If you suspect or have reason to believe somebody knows any of your passwords, you must contact IT Services who will assist in changing your password(s). IT Services can request your network password for instance when re-building your laptop but you have the option to go back afterwards and change the password. This can be done by logging into Windows then pressing CTRL + ALT + DEL and selection the **Change a password** option, you can then select a new password which must be a minimum of 8 characters long and contains at least once capital and one number.

2 Software installation.

Your device(s) and the software installed on them have been tested to ensure they work together correctly. The devices rely heavily on the software installed on them to function correctly. The device can be easily compromised and rendered non-operational by the incorrect or inappropriate installation of software.

2.1 You must not install any software which is not connected to your work as an employee at the school.
2.2 You must not install any software which you do not have a valid licence for.
2.3 You must not install any software from sources you do not know or trust.
2.4 You must not purchase any software, all software purchases must come through IT Services for financial auditing and asset ownership purposes. If for example you purchase an iPad App using your personal iTunes account and payment card these will not be reimbursed by the school as the ownership cannot be transferred from you to the school.

Given the complexity of today's software it would be better to have any software you require installed correctly by IT Services.

3 Device handling.

Incorrect handling of your device(s) will greatly reduce its operational effectiveness and possibly cause injury to yourself or others. The following guidelines are meant to advise on the main points and are not a complete definitive list covering every eventuality. Should you be in any doubt or require clarification then please contact IT Services.

3.1 **Charging.** Chargers should be plugged into the wall socket, the power then switched on and then the charger cable inserted into the device. Storing the charger away correctly after use is very important, the wires of the charger must not be wound around the charger block as this will cause the wires to become damaged causing premature failure of the charger.

3.2 **Batteries.** Devices where rechargeable batteries are fitted perform best when run on complete charge/discharge cycles. That means you should allow the battery to fully charge and then use the device until it advises you to switch to mains power to charge. This procedure will greatly lengthen the life of the battery and reduces the need to rely on the charger on periodic daily basis.

3.3 **Protective Cases.** If your portable device has been supplied with a protective case and covers these must be used, failure to do so may render any insurance null and void and the full repair/replacement cost will have to be met by your department.

3.4 **Removing laptops from bags.** You must use both hands when taking the laptop out of the laptop bag and not try to juggle this task with others. The laptop should never be switched on and used with it inside the laptop bag as the air vents on the sides and underside of the laptop will be blocked. This will cause the laptop to overheat causing problems such as programs crashing and in some cases it has been known for laptops to catch fire.

3.5 **Opening your laptop.** You should use both hands; one hand should be used to securely hold the base (lower half) of the laptop. While the other should be used to slide the central catch (where fitted) and raise the laptop lid from the centre edge. The lid should not be pulled up using the corners as this is the weakest point and will weaken the screen hinges and possibly cause the screen to crack due to uneven stress being applied.

3.6 **Closing your Laptop** You should gently close the laptop using the top centre edge of the screen lid. Using the corners of the laptop lid to close it will cause undue stress to the screen and the hinge mechanism causing premature failure. Under no circumstances should you place any paper or other objects (e.g. pens) on the keyboard area as this will distort the screen hinge mechanism and in many circumstances (e.g. pens) cause the screen to crack.

3.7 **Powering down your laptop.** Your laptop should be shut down form Windows when transporting to and from home or when not being used for more than one lesson. When you are moving between lessons it is best to close your laptop screen lid, this puts the laptop into standby mode (allowing for quicker start up). In either situation you must not place the laptop into the bag until the laptop has powered down (screen off and fans have stopped moving).

3.8 **Storing portable devices in a laptop bag.** When placing portable devices into the laptop bag, ensure that none of the cables or anything else you have plugged in (e.g. USB Memory sticks) are attached. Leaving devices attached will result in premature failure of your device due to excess stress being applied to the ports during transport.

3.9 **Carrying your laptop**. You have been provided with a laptop bag which has a sole purpose, to allow you to transport your laptop safely and securely from one location to another and to help prevent it from getting damaged. The laptop bag should be used for this purpose only and not for storing others things such a stationary. You should not move the laptop around the building with the screen lid open, this is a health and safety hazard where you could endanger yourself and others.

4 Wireless access.

There is a wireless network deployed around school. Given the nature of wireless technology and the building infrastructure there maybe places where there is little or no wireless coverage. In order to alleviate problems associated with lost wireless connections you are advised to;

4.1 **PC Logon Wait Time**. When Windows loads up and you are presented with the Windows logon box, wait at least 1 minute before logging in. This gives your laptop time to find the wireless network and establish a connection. If you do not do this you will be able to logon but will find you cannot access network resources. This is because network resources such as ‘drives’ are connected at logging in time and then only once a network connection has been found/established. The same waiting period should be adopted for laptops that were in standby mode as the laptop has to find the network again. Failure to do this will require you to log out and log back in again.

4.2 **Close applications.** Shut down applications (e.g. SIMS) before closing the laptop lid. Windows applications 'detect' the presence of network connections and can crash if a connection to the network is lost. Network connections are easily lost by the computer going into standby/power saving or by walking through an area with the laptop open which has little or no wireless coverage. The only effective way to overcome a crash problem once it has occurred is to restart the laptop.

4.3 **Coverage.** For areas where wireless coverage is insufficient you can request a network cable for your laptop. This cable should be connected before switching on the laptop or bringing it out of standby mode. If you do not do this Windows may bias towards the poorer wireless signal regardless of the cable being connected.

4.4 **Speed.** Wireless speeds provided by the school network runs at maximum of up to 350Mbps once networking overheads are taken into account. This connection is shared by all users within the area. You should not expect the same performance from wireless as you do from machines which are connected by a network cable, as cabled devices run at a dedicated 100Mbps per user.

5 Saving work.

You are solely responsible for ensuring your files/work are saved in the correct locations (if in doubt consult IT Services). Files saved on the school network should be work related, this is because the school storage servers have a limited amount of disk space which has to serve the whole school needs. We rely on the staff to manage their files appropriately taking into account why network storage space is provided.
To assist with file management the following points may prove helpful;

5.1 **C Drive.** The C drive is the main storage disk inside your PC/laptop, this is where the computer keeps all the files it needs to run. The C drive is **not backed up** and should the physical disk inside become damaged all files on it may be lost. The C drive should only be used for installing programs like those provided on CD-ROMS. In the event that the laptop disk is damaged beyond recovery it can be replaced and the software reloaded using the CD-ROMS.

5.2 **H Drive.** The H drive (My Home Drive) is your personal storage space on the network where you should store the files/work you create. The H Drive is synchronised with your laptop and is available to you when you are away from the school network. You should never store any sensitive or confidential files in this drive. Files saved in the H Drive are periodically backed up.

5.3 **P Drive.** The P drive (Confidential drive) is your personal storage space on the network where you should store confidential and sensitive files. Files stored in this drive are not accessible by you outside school. You should never take sensitive data which can be used to identify people off site unless the data is encrypted (the school can supply encrypted memory sticks where department heads have requested them for their staff). Files saved in the P Drive are periodically backed up.

5.4 **X Drive.** The X drive (Staffshare) is a school staff storage area where you can place files to be shared by other staff within the school. You are responsible for ensuring any file(s) you place into the X drive are relevant and must delete the files when they are no longer required. Files saved in the X Drive are periodically backed up.

5.5 **Hand in Work folder.** The Hand In Work folder is where pupils may place work which is too large or complicated to upload into SharePoint. Once a pupil places a file into the Hand In Work folder they cannot delete or edit it. It is your responsibility to ensure that once the work has been marked it is either deleted or if required for examination/coursework reasons it is archived onto DVD. IT Services can assist in providing archiving to DVD but you will be responsible for the disc(s) once handed over.

5.6 **SharePoint.** The school SharePoint site is a work platform designed for sharing documents between staff and pupils. You must never place any sensitive or confidential files onto the SharePoint site as this is accessible from outside of school.

5.7 **Google Drive.** You can use your Google drive as a personal storage drive (it currently has unlimited storage) to save school work which can be accessed anywhere in the world. Please note the unlimited storage policy may be subject to change at some point in the future by Google. The school has no control over backup procedures or infrastructure that runs Google drive. Google drive must not be used to store any sensitive or confidential files.

6 Internet and email usage.

The school internet service provider, logs and filters all internet traffic to/from the school. You should not expect your internet or email activity to be private as the school, police and security agencies have the authority to request this information. If you are unsure about how you should use your internet and email accounts please seek guidance from IT Services.

6.1 **Email Communications.** To protect yourself and maintain your privacy you should never use or disclose your personal email address for any school related work. You must only use your school provided email account to communicate with staff, pupils and external parties on matters directly connected with your work as an employee of the school.

6.2 **Internet Access.** You have been granted internet access so that you can perform your duties. It is therefore expected that your online internet activities will reflect this. The school does however recognise that staff should have some freedom to use the internet for non-teaching activities. The school cannot provide an exhaustive list on what types of activity are acceptable. Instead you are directed to apply reasonable judgement for any activity you undertake so that it is appropriate for a school environment and if discovered would not bring the school into disrepute.

Conclusion

If you are unsure about anything contained within this document or require further clarification on ICT related matters not already covered you are directed to contact IT Services who will provide guidance as appropriate. A copy of this ICT Resources Guidance Document will be given to you at the time of your ICT resources being issued to you for your records.

Declaration

I understand the information presented above and have been shown how to take care of my devices and it's accessories. I also confirm I have a received a copy of this document and I sign below to declare this.

Signed (+ Print Name) ________________________________ Date _________________

Issued by (+Print Name) ________________________________ Date _________________