



# Online Safety Policy

Last Reviewed	November 2024
Next Review Date	November 2026
Ratified by the Trustee Board	November 2025

# Online Safety Policy

## I. Context

The primary function of ICT deployment in the school is to facilitate learning, primarily in the classroom but extending to the home. The school further deploys ICT for its core day-to-day administration activities and to help make informed strategic decisions.

This deployment links closely to the aims of the school which are to:

- Develop lively, enquiring minds capable of original thought and well-balanced critical argument.
- Develop confident, independent learners well-equipped for lifelong learning.
- Allow students to derive enjoyment from their learning which should extend their intellectual capacity, develop their interest and stimulate their curiosity.
- Embrace the many opportunities afforded by developments in ICT, whilst fully accepting the responsibilities that go with using them properly.

This policy reflects the school values and philosophy in relation to the safe teaching and learning of, and with, ICT. This policy is intended for:

- All teaching and support staff.
- Visitors and letting customers.
- School Trustees.
- Parents and guardians.

The policy applies to everyone who uses any device, account or service issued by the school; online service operated on behalf of the school.

The agreements (included in this policy) and their implementation will promote positive behaviour, promote our character builders and enable lifelong learning.

Any member of staff found to be in breach of the guidelines may be subject to disciplinary action. Any student in breach of these guidelines will face appropriate school sanctions.

21st Century learners live in fast moving ever-changing world where the amount of information and knowledge is growing exponentially. Teachers can no longer be seen as the 'font of all knowledge' as students can access huge amounts of information/knowledge at the click of a button. The role of the teacher as an experienced facilitator is key; guiding students to explore, think and learn for themselves, whilst on this journey developing the critical skills to:

- **SEARCH** for relevant information and knowledge.
- **ASSESS** the validity, reliability and bias of that information.
- **EVALUATE** material.
- **PROBLEM SOLVE** to find solutions logically.
- **SYNTHESISE** information.
- **CREATE** and **DEVELOP** their own material.
- **ENABLE** them to stay safe online.
- **ADAPT** to and **EMBRACE** a constantly changing technological world.

## 1.1 Risks

The breadth of issues classified within online safety is considerable, but as outlined by KCSiE 2025, they can be categorised into four main areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm/abuse; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying). For child on child abuse, see the Safeguarding and Child Protection Policy.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and /or financial scams.

KCSiE 2025 also gives the following risks: **Misinformation, disinformation, and conspiracy theories.** These are now explicitly included under the "content" category.

We believe that online safety is an essential part of our safeguarding responsibility. That students and staff should be empowered to build resilience and develop strategies to manage and respond to risks appropriately online.

We achieve this by educating students and staff in key areas of e-safety such as:

- How to identify online dangers and avoid them.
- How to report online abuse or material that makes them uncomfortable.
- How to safely and professionally interact with other people online. So that their conduct does not harm, upset other people or bring into question their motives.
- Being aware that their online actions not only affect them but can also negatively impact on their family, friends, school and the wider community.

The school accepts that students and staff will have access to privately paid for unfiltered and unmonitored internet access via home broadband and mobile data plans (e.g. 3G, 5G) which we cannot control but through e-safety education we can empower students and staff to stay safe and act responsibly.

In recent years there has been a proliferation in the home of internet connect devices that students and staff have access to, such as laptops, mobile phones, tablets and gaming consoles. The school recognises the importance and value of these devices not only in an educational context but in a recreational one.

Many of these devices are used in both contexts thus blurring the line between the two. By educating our students and staff in e-safety we are giving them the knowledge and skills necessary to stay safe, respect others and adopt behaviour and language appropriate on how the devices are being used.

## 2. Aims

We aim for all students and staff in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which will enable them to use appropriate ICT resources effectively as powerful tools for teaching & learning.

Our students and staff need to be comfortable with and skillful at navigating ICT. To fulfil the above aims it is necessary for the school to ensure that:

- There is sufficient quality access to ICT equipment, software and online learning environments.
- ICT experiences are focused on enhancing learning.
- Appropriate ICT skills and e-safety knowledge is taught and embedded in the curriculum and wider curriculum. Delivered primarily through the ICT and Computing curriculum lessons.
- Everyone who uses the school's ICT understand how to be safe (including personal safety, security of data etc.)
- The school works in partnership with parents and educational services providers to help keep students safe.
- The school ensures to the best of its endeavours that students and staff are kept safe from inappropriate material (web filters and anti-virus) and that the school is vigilant at monitoring students and staff online activity through activity reports.
- Cross curricular links are exploited where appropriate
- The school keeps up to date with Artificial Intelligence and seeks ways to safeguard students and staff with its ever increasing use in wider society.

This policy aims to outline procedures for the safe use of ICT and the online world by staff and students.

The policy will define the code of conduct for students and staff when online and when using related technologies, and provide online safety guidelines.

The policy aims to raise awareness of good e-safety practice focused upon the value and benefits of using ICT and related technologies, whilst being mindful of the possible risks and dangers involved.

The policy outlines the responsible approach adopted to educating students in online safety/digital literacy through a broad, relevant and progressive curriculum.

This policy is available on our website for access by parents/carers, staff, students and wider stakeholders.

**This Policy and procedures have links to and should be read in conjunction with our other policies and procedures outlined below:**

- Anti-bullying Policy
- Positive Behaviour Policy
- Child Protection Policy
- PSHCE and Relationships and Sex Education Policy.
- Mobile Phone Procedures
- Managing Staff Allegations
- KCSiE 2025.
- Guidance for Safer Working Practice, Feb 2022,

## 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 be or cause to be a serious safeguarding issue.
- It may involve breaking the law and therefore illegal.
- It may result in poor or unacceptable behaviour.
- 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.
- Staff, visitors, parents/carers and students can be involved or affected.

## 3 Evaluation

The Policy will be evaluated by the Headteacher annually to ensure it is still fit for purpose. Circumstances may require more frequent modifications for example it will be promptly reviewed in the following instances

- Serious and/or frequent breaches of the Acceptable Internet Use Policy or in the light of online incidents.
- New guidance by government/local authority/safeguarding authorities.
- Significant changes in technology as used by the school or students in the wider community.
- Online incidents in the community or local schools which might impact on the school community.
- Advice from the police and/or local safeguarding children partners.

## 4 Authors

This policy has been reviewed by the Designated Lead for Safeguarding (DSL) (Sarah Nowell) who initially wrote the policy in conjunction with the teaching ICT department and the IT Service Delivery Manager. It considers the:

- DfE statutory guidance Keeping Children Safe in Education 2025 (KCSiE)
- Meeting Digital and Technology Standards in Schools and Colleges (DfE March 2023)
- Leeds City Council Guidance for staff working in educational settings on the Use of Digital Technologies and social media 2020.
- Teaching Online Safety in Schools DfE June 2019.
- Guidance from CEOP (Child Exploitation and Online Protection).
- Sharing Nudes and Semi Nudes – UK Council for Safer Internet
- When to Call Police
- Generative AI: The guidance from the DfE for using generative AI, 2025

## 5 Appendices

The following appendices are used to support these procedures:

Appendix 1.	Roles and Responsibilities
Appendix 2.	Education and Training Approaches
Appendix 3.	Safer Use of Technology

Appendix 4.	Staff Expectations
Appendix 5.	Social Media
Appendix 6.	Mobile Phones
Appendix 7.	Responding to Online Safety Incidents and Concerns
Appendix 8.	Procedures for Responding to Specific Online Incidents or Concerns
Appendix 9.	Confidentiality
Appendix 10.	Equal Opportunities
Appendix 11a.	Acceptable Use Agreement for Students
Appendix 11b.	Acceptable Use Agreement for Staff
Appendix 12.	Safeguarding for Remote Learning
Appendix 13.	ICT Resources Guidance Document
Appendix 14	Filtering and Monitoring
Appendix 15	The use of Generative AI

## **Appendix I: Roles and Responsibilities**

### **1a) The Leadership and E-learning specialists will:**

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Named staff will be aware of the procedures to follow in the event of a serious online allegation being made against a member of staff.
- 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 there is online safety training for staff as part of CPD through the code of conduct and cyber security module, through annual Safeguarding training and at induction.
- Ensure that effective and appropriate filtering and monitoring systems are in place and ensure that the schools systems meet the standards as outlined in KCSiE and Meeting Digital Standards DfE March 2023 guidance and generative AI guidance, 2025.
- Work with IT 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.
- Work together to review systems annually and produce the online safety report.

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

- Act as a named point of contact and will be day to day responsible for all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Have overall leadership and responsibility for filtering and monitoring as outlined in KCSiE 2025.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate. Have a lead role in main policy development.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and know how to report issues.
- Work closely with the ICT Teaching specialists, Data and IT Support Teams in school to set up systems to help control and monitor usage so students and staff are safeguarded.
- Lead on the review of school systems and write the annual online safety report.
- Will receive reports of incidents and keep a log
- 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, using CPOM's as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the Leadership Team and the Trustee Board.
- Work with the Leadership Team to review and update any online safety procedures.

**Ic) It is the responsibility of all members of staff to:**

- Read, understand and adhere to this Policy and the Acceptable Use Agreement. Being aware of practice and procedures for reporting online incidents, including online risks.
- Follow and adhere to the staff expectations and procedures within this policy which includes personal use, off site use, school use and professional online conduct.
- 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 into curriculum delivery where possible.
- Rigorously monitor pupil internet and computer usage in line with policy. This includes Digital Cameras, i-Pads and other technology.
- Ensure that when ICT is used it has a specific learning purpose to help meet/deliver lesson objectives. Pre-vet websites used in lessons for suitability from a safeguarding point of view as well as a value-added learning prospective.
- Promote best practice regarding avoiding copyright infringement and plagiarism.
- Promote student skills to critically evaluate propaganda, fake news, fraud, phishing, and scams.
- Identify online safety concerns for either staff or student and take appropriate action by following the school's Safeguarding policies and procedures.
- Know when and how to escalate online safety issues.
- Take personal responsibility for professional development in this area.

**Id) 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 Policy or Procedures, including the procurement and management of effective filtering and monitoring systems, reviews and all aspects of technical support
- 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.
- Monitor and report any filtering breaches to the DSL and Leadership Team, as well as, the school's Internet Service Provider or other service providers, 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.
- Prepare reports for the Child Protection team, Trustees and Leadership team.
- Attend and co-lead online safety meetings.
- Train staff and Trustees in matters of filtering and monitoring

**Ie) It is the responsibility of students to:**

- Engage and adhere to the age appropriate online education as instructed by the class teacher and to engage in safety education opportunities within or outside of the classroom.
- Contribute to the development of our Online Safety Procedures.
- Read and adhere to the school expectations within the Acceptable Use Agreement.
- To adhere to the Mobile Phone Policy.
- To understand the positives of online technologies and also the potential dangers and risks.

- To understand that misuse of social media can damage reputation and relationships. That it can impact widely on staff/students/community and can be classed as cyber bullying or linked to illegal activity such as sexting.
  - To care for any loaned school equipment and return it in the condition given.
  - Respect the feelings and rights of others both on and offline.
  - Take responsibility for keeping themselves and others safe online. Report misuse, harm or concerns.
  - Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues. Be aware of the click CEOP reporting tool.
- Students bring their own any personal device or phone at their own risk and are held responsible for this. School does not accept responsibility for loss, theft or damage.

**If) It is the responsibility of parents and carers to:**

- Read and understand 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.
- Monitor online activity and behaviours if children are subject to remote learning, ensure children are in a suitable environment, fully dressed and ready to learn.
- 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 any online services provided by the school safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- Read the information the school sends home about online safety and make use of the information and signposting on our website.
- To set parental controls and monitor their children's usage including content and contact.
- To ensure that generative AI is not used in a child's assessment, school work or homework in order to cheat, copy or plagiarize or claim false recognition and authorship.

**Ig) It is the responsibility of Trustees to:**

Ensure this policy is regularly reviewed and approved by the Headteacher to ensure it remains current in line with trends and formal guidance. Ensure the adoption and implementation of this policy within school. Trustees will receive updates about on-line safety within Safeguarding reports. A member of the Trustee Board is appointed to the role of Safeguarding Trustee. The role will include regular meetings and action planning with the DSL, regular monitoring of filtering systems and checks and reporting to the relevant Committee meetings.

The Trustees are specifically responsible for:

- Managing, reviewing, promoting and evaluating adherence to online safety policies.
- Ensuring that there are mechanisms to support pupils, staff and parents facing online safety issues.
- Ensuring that the DSL is trained to support staff and pupils and to work with other agencies.
- Ensuring that all staff receive relevant training that is refreshed.

- Educating parents and the wider school community.
- Liaise with the DSL, HR department and Senior Leadership Team (SLT) with regard to reports on online effectiveness, incidents and monitoring. Complete a safeguarding audit /report.
- Hold the school to account for its filtering and monitoring processes and systems
- Discuss and analyse the annual online safety report and AI processes as they evolve.

The school has appointed Tessa Freer as having responsibility for online safety.

## 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 PSHCE, 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:

- Reminding pupils of online safety at the start of ICT based lessons.
- 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 through drop down sessions, themed weeks and national days
- Using support, such as external visitors, where appropriate, to compliment and support the school's internal online safety education approaches i.e., Police Liaison officer

### 2b) Teaching and Learning through ICT

Online safety is integrated into the curriculum in every circumstance where ICT is being used, and during Personal, Social, Health, Citizenship & Economic Education (PSHCE) lessons where modules relating to: managing risk and personal safety/ social influences/ media literacy and digital resilience is being taught. (refer to the school's Relationships and Sexual Health Education Policy (RSE) for further details with regards to the taught curriculum and specific E and online safety education).

Through ICT/Computing/PSHCE/RSE lessons students will be taught about the possible risks and dangers that they might encounter when using the internet and personal devices such as laptops, mobile phones and gaming consoles. The breadth of issues covered within the taught curriculum can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful materials. Including misinformation, disinformation, and conspiracy theories.
- **Contact:** being subject to harmful online interaction with other users.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce:** being at risk from online gambling, inappropriate advertising, phishing and/or financial scams.

Students will be taught (age and stage appropriately):

- How photographs can be manipulated.
- The importance of keeping personal information private.
- About safe social networking and chat rooms.
- Ownership of personal images and the risks sharing intimate nude and semi-nude images.

- What constitutes a healthy relationship online.
- The characteristics of abusive behaviours online.
- Awareness of exploitation both sexual and criminal.
- The skills to challenge or seek support for financial exploitation online.
- How to develop media literacy and digital resilience and understand the pro's and con's of AI.
- The implications of inappropriate posts on career progression and employment.

The internet is used in to raise educational standards, promote student achievement, support the professional standards of the work of staff members and to enhance the school's management functions. It is the responsibility of every staff member to equip students with the necessary ICT skills, transferable knowledge and awareness to enable them to make outstanding progress, fulfil their potential and secure further and higher education, apprenticeships and/or employment.

Students will have access to ICT and online safety information as part of their ICT curriculum, and/or via access to the ICT where they can access a number of teaching and learning resources. To enable students to expand their horizons they have unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries and can contact schools in other countries resulting in cultural exchanges between students all over the world. This is supported by internet security, web filtering and pre-exchange checks.

Teaching and Learning is enriched by access to subject experts, role models, inspirational people and organisations and an enhanced curriculum this includes:

- Interactive learning tools.
- Access to case studies, videos and interactive media to enhance understanding.
- Collaborative activities, locally, nationally and globally.
- Self-evaluation.
- Feedback and assessment.
- Updates on current affairs.

ICT can be used to give students the freedom to be creative and the opportunity to explore the world and its differing cultures from within a classroom. It can be used as a tool for social inclusion and provide personalised access to learning.

For members of staff ICT can aid professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies. It can allow professionals to access professional support through networks and associations. It is a communication tool which gives professionals the ability to mark and assess student work and provide immediate feedback to students and parents/carers. It is also an administrative instrument used for class management, reporting, attendance records, collaborative working, and assessment tracking.

## **2c) Learning to Evaluate Online Content**

There is a multitude of information available online and it is important that students learn how to evaluate internet content for accuracy and intent. Students are taught to become digitally literate across the whole curriculum and are encouraged to be critically aware of materials they read, and how to validate information before accepting it as accurate. Students will be taught to understand the bias of web authors, separate fact from fiction and practice etiquette on the internet, emails and social media.

Students learn how to use age-appropriate tools to search for information online, how to acknowledge the source of information used and to respect copyright.

Plagiarism is against the law and the school will take any intentional acts of plagiarism seriously. Students who are found to have plagiarised will be disciplined in accordance with the Positive Behaviour Policy. If plagiarism has occurred during an exam or a piece of coursework the student may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites, then the URL must be reported to the teacher (for students) or IT Support Staff.

## **2d) Remote Learning**

If the school reverts back to remote learning the school teaches a “planned and well-sequenced curriculum so that knowledge and skills are built incrementally” and has systems in place for “checking, daily, whether pupils are engaging with their work”.

The schools named senior leader (Zoe Comiskey) has overarching responsibility for the quality and delivery of remote education, including that the provision meets expectations for remote education.

The school uses Google Meet and the Google Classroom digital platforms for remote education and meetings; these “will be used consistently across the school”. These platforms can be interactive, assessed and staff can provide feedback and our staff are “trained and confident” in its use”.

We follow the following Guidance, Remote Education Good Practice:

<https://www.gov.uk/government/publications/remote-education-good-practice/remote-education-good-practice>

(See Appendix 12: Safeguarding for Remote Education)

## **2e) Vulnerable Pupils**

The school is 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.

The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students. Within the school the SEND team has responsibility for providing bespoke support to students in the event of remote learning. We have a TLR holder for EAL students support.

## **2f) Training of Staff**

The school through the DSL will ensure that:

- That as part of the staff induction programme new starters are made aware of the safety procedures within the scope of Child Protection and Safeguarding Awareness.
- Up-to-date and appropriate online safety training is made available and undertaken by all staff on an annual basis. This will cover the potential risks posed to pupils (Content, Contact, Conduct, Commerce) as well as professional practice expectations.

- Staff are made 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.
- Staff are made 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.
- Staff have a code of conduct training, and they have read and understood key documents such as Keeping Children Safe in Education (KCSiE) and Guidance for Safer Working Practice.
- 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.
- Support and signpost staff who are affected by online misuse or abuse. Ensure staff can signpost students.

## **2g) 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, email updates and information on the school's website.
- 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, including access to:

- Computers, laptops, i-Pads and other digital devices.
- Filtered internet with access to search engines and educational websites.
- School website, Microsoft365 and Google Classroom work and learning environments.
- Email through Microsoft365.
- AI for teaching and learning for staff only, using approved educational versions of Google AI (Gemini) and Microsoft Co-Pilot/ChatGPT.

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.

Teachers will use search tools to identify the best age appropriate learning resources that meet the requirements of their learners.

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.

The school supervise pupils appropriately according to their age and ability.

### **3b) Managing 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 Agreements.

### **3c) Internet Filtering and Monitoring**

The Leadership Team have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks. This is reviewed and checked regularly. Leadership 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 e.g. unblocking a website 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. 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's internet service provider (ISP) EXA Networks provides the school with broadband connectivity that meets the legal requirements, and which is tailored for use in schools.

EXA Networks uses the SurfProtect Quantum+ web filtering platform to monitor all web traffic in and out

of school. EXA Networks blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The SurfProtect Quantum+ platform blocks all sites on the [Internet Watch](#)

**Foundation** (IWF) list. In addition, the school uses the Sophos Anti-Virus platform on all school laptops and PC's which will attempt to block access to questionable sites e.g. pornographic. The Sophos anti-virus continues to work on school devices even when away from school.

EXA Networks is a member of the Internet Watch Foundation (<https://www.iwf.org.uk/membership/our-members/exa-networks> )

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 IT 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 in addition to our ISP which can manually add them to filtering system.

### **3d) NetSupport Classroom Cloud**

As an additional layer of protection all school computers and laptops have Classroom Cloud software installed on them. The Classroom Cloud software monitors all activity undertaken on computers and any activity that the software deems to be a risk or concern is captured with a screenshot and an alert is generated in real time. These alerts can be reviewed by designated staff (Behaviour Support and IT Services) and appropriate action taken.

### **3e) 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. The schools Data Protection Officer is the HR Manager (Lauren Robinson).

### **3f) 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.

### **3g) Passwords**

To access the school network, certain installed applications and email all users are given a unique username and private password. They are responsible for keeping their password private.

Access to online websites, learning platforms and services used by the school can result in a mix of bespoke usernames/passwords and shared usernames/passwords. These are advised to users as appropriate with the understanding that they must not share:

- Unique usernames and passwords with anyone else.
- Disclose shared usernames and passwords with anyone outside of school.

Users are required to use strong passwords and not write them down where they may become easily discoverable by other people.

### **3h) 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.

### **3i) Creation and Publishing of Images and Videos**

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.

#### **Using photographs of students**

- Before anyone can create or take photographs or videos they must first have authorisation from the school. Before this authorisation is granted the following conditions must be satisfied:
  - That parental/carer consent has been granted (by use of an opt out method at Admission). Staff need to check this each time.
  - That published images do not put students at risk.
  - That the school has the ability to have removed pictures at a future date should new information come to light.
- Personnel recording devices must not be used to record or store images of students.  
Only images created by or for the school will be used in public and students may not be approached or photographed while in the school or undertaking school activities without permission.
- Electronic and paper images of students will be stored securely.
- All images of students are processed and stored in accordance with the General Data Protection Regulation 2018, and following GDPR and Data Security regulations.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- When images are used for public documents, including in newspapers, full names will not be published alongside images of the student.
- Events recorded by family members of the students such as productions or sports events must be for personal use and only at the discretion of the school.
- Students are encouraged to inform a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or photographs that they are being asked to participate in.

- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour. They will wear identification at all times, will not have unsupervised access to the students and will be supervised by a member of staff.
- Child Protection designated officers are aware of students who need protection and who would be put at risk if their image is used and will ensure that members of staff are made aware of students who cannot have their image published in any form.

### **3j) 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.
- Students have limited access to who can contact them via their school email account. This list is held as an email rule on the Microsoft email server, email addresses not on this list will automatically be rejected and neither the student nor the sender will be made aware. Staff may request from time to time that rule be updated e.g. when a new learning website/platform is used and the provider needs to send information to students. All requests to update this rule have to be made via email so a record is kept, requests from students will not be accepted.

### **3k) Management of Learning Platforms (VLE's)**

The schools official learning platform is Google Classroom which is supplemented with Microsoft365 and other subject specific third-party platform providers to make up a bespoke set of virtual learning environments (VLE's).

- Leaders and staff will regularly monitor the usage of these, in particular, message and communication tools and publishing facilities.
- Only current staff and students will have access to these platforms. When staff and/or students leave the school, their account or rights will be disabled/deleted.
- Students and staff will be advised about acceptable conduct and use when using these VLE's.
- All users will be mindful of copyright and will only upload appropriate content onto these VLE's.
- Any concerns about content on VLE's 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 VLE(s) for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement. i.e. A student's parent/carer may also 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.

### **3I) Management of Applications which Record Children's Progress**

The school uses SIMS, CPOMs, Class Charts and SISRA to track pupil 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 applications that record and store students' 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: Staff Expectations**

### **4a) Aims**

The expectations' regarding safe and responsible use of social media applies to all members of Horsforth School, but these are specific for staff. Our expectations are intended to guide, advise and support staff; to protect staff, students, the school and wider community.

### **4b) General Expectations**

The use of computer systems without permission or for purposes not agreed could constitute a criminal offence under the Computer Misuse Act 1990.

Staff members should act responsibly and with an awareness of the consequences of their actions. Staff members must act with the best interests of students at all times.

Staff who are provided with a laptop or other computing device must use this only for academic purposes, these remain the property of the school and are open to scrutiny by Senior Leaders.

All staff members are responsible for their personal use of social media, networks and electronic devices and are expected to ensure that any use of such technologies does not breach the schools safer working practice or undermine the reputation of the school.

Staff are personally responsible for the security and privacy settings when using social media and networks and failing to ensure that privacy settings are secure could lead to a disciplinary process if the content breaches professional expectations.

Staff must ensure that their use of ICT and social media is professional at all times, even if this is outside of the working day, and that behaviour which breaches could breach the Code of Conduct could lead to disciplinary action.

All contact made with students must be made through appropriate school based channels, such as school email or Google Classroom, and should be made within clear and transparent professional boundaries and only made with regard to matters regarding the school.

Staff must not give out personal details, such as telephone numbers, email addresses, social media identities to students, ex-students or parents/carers of students.

Any contact made with ex-students should not be made if they are under the age of 18, are currently a student at the school or in full time education. Great caution should be advised with regards to any contact with any ex-students and staff members must use their personal judgement and be mindful of their professional standing.

Any member of staff found to be in contact with students, and ex-students in this way, without consent from the Headteacher, may be subject to disciplinary action.

Staff should be aware that when giving information or reprimanding students they should do it in a tone or manner which they would be happy for a parent/carer to witness. Please be aware that due to the development of smart phone technologies recording of dialogue between staff and students is an increasing possibility.

Safe and professional behaviour of staff online will be discussed at induction training. This relates to the use of social networking sites outside of the working environment. As a school employee it is important to be aware that posting information or views about the school cannot be isolated from your working life. Comments about the school, students, parents/carers or colleagues can bring the school's reputation into disrepute and make both the school and the employee liable to legal action.

### **4c) Appropriate Computer Usage**

Staff members are expected to use computers in lessons only for teaching and learning and not for other work.

Staff must ensure that students are unable to access activities and information on the computers that is not relevant to teaching and learning and the lesson.

Staff must log off or lock their computing devices when not in use to protect confidential and personal information.

Only members of IT Services should move computer equipment, unplug cables or remove screws or covers from equipment and upload/download or copy programs and change, or attempt to change the configuration of any computer.

Students should not use computers in classrooms without permission or without a member of staff being present, specifically at non-contact times, to ensure that staff members are able to supervise online access and secure equipment.

#### **4d) Social Media and Networks**

Staff members should not be in contact with students, ex-students under 18 years in full time education or parents/carers of students using social media and networking, unless prior permission has been given by the Headteacher (or you have known them previously on a personal level before they started at the school and the Headteacher is aware).

The school does not recommend that staff are in contact with any ex-student (over 18 years) or parent/carer on social media.

Students should not be added as friends and staff must not respond to friend requests. If a member of staff suspects that an existing friend is a student or a student is using another name to befriend the member of staff the friendship should be ended and this should be reported to the Headteacher immediately.

If a member of staff coincidentally has a contact established with an ex-student, parent/carer or student the member of staff must use their judgement and regulate or stop this contact. If a student, ex-student or parent/carer persistently attempts to befriend a member of staff this should be disclosed to the Headteacher.

The use of personal social networking activity is at the discretion of the individual, however the professional responsibilities of the individual need to be considered in all postings.

It is important to ensure that your personal information is secure and that high strength passwords are used and that profile settings are restricted. It is advisable to log out of social networking sites when not in use as a security precaution.

Staff must be aware of how to set privacy settings on their profile and be mindful that some social networking sites revert to default settings when an update is made to their service. Staff should be vigilant to any changes in their profile privacy settings.

Professionals should consider what information they use for their profile, for example the photograph and the amount of personal information that is displayed. Profiles should not identify your employer or place of work.

Staff should not publish school information or their school email address on a personal social networking site, or use this address as part of your login/registration on a personal site.

All postings on social media and networks should be considered to be in the public domain so staff members should consider this when making decisions about the content of social media activity.

Any material which is posted on social media and networks which is considered to bring the school into disrepute or is considered to put students or staff at risk of harm will be dealt with under the schools Disciplinary Procedures and follow the Allegations Management Policy (if applicable).

Staff members should not make reference online to any students, parents/carers, colleagues or to any work-related issue. This also includes posting photographs or videos online which identify your place of work, or any students and parents/carers.

While access to social media sites through the school network is blocked to employees, accessing the internet through mobile phones and other mobile devices is prohibited, without prior approval from the Headteacher, during working hours. Staff members should never use school networks or equipment to access or update a social media site, unless this is with prior approval, for example to post on Twitter or Facebook account.

#### **4e) Facebook, Twitter and similar social media advice**

To ensure that staff are safe and protected as professionals:

- Keep your profile picture post modest. Remember students can still search for you and see your picture without being your friend.
- Create your photo albums with privacy settings so only your friends can see them.
- Reject all friend requests from students. You do not need to report this unless it becomes a recurring problem. People are not notified when you reject their friend request.
- Use the Facebook/Twitter privacy settings to limit who can see your full profile. Set it so that only friends can see everything like your pictures, your wall, and your personal and contact information.
- Use limited public information about yourself on your profile. For example, address, email, date of birth, contact telephone numbers do not need to be shown to everyone, they can be privately messaged if needed.
- Do not use your school email address as your email contact.
- Report any threats of violence or other inappropriate posts/images to Facebook or to the relevant authorities, such as the Child Exploitation and Online Protection Centre (CEOP) or the police.
- Customise your privacy settings. Limit what people can see
- Don't ever announce on your wall that you are going away. Many cases of burglaries are supported through these disclosures on Facebook and Twitter.

#### **4f) Internet Use**

All staff sign an Acceptable Use Policy Agreement which details the expectations placed on staff, which are outlined within this policy.

As a general principle, internet access is provided to employees to support work related activities. The following list is not intended to be an exhaustive list, but sets out broad areas of use that the school considers to be acceptable uses of the internet.

School web filters are assessed annually as a minimum against the <http://testfiltering.com/> website as recommended by the UK Safer Internet Centre, the certificates/screenshots for these tests are then stored for records. The tests are also carried earlier if we have a major change to web filtering or a change in KCSiE / Government guidance.

Examples of acceptable use include but not limited to:

- Using email to communicate with other staff and students on matters related school activity.
- Using email and School Comms to communicate information to Parents and Carers.
- Find, evaluating and using websites and other online resources for use within lessons or to assist in the administrative activities of the school.

Examples of unacceptable use (irrespective of how or where they are carried out) include but not limited to:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy.
- Use for racial, sexual, homophobic or other harassment of individuals.
- Access pornographic, obscene or illegal material.

- To solicit personal information with the intent of using such information to cause emotional or physical harm.
- Entering into a commitment on behalf of the school (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic, extremist or otherwise illegal material.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into networks and accounts.
- Publishing defamatory and/or knowingly false material about school, colleagues and/or our students/parents on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information in a personal online posting, upload or, transmission, including financial information and information relating to our students, staff and/or internal discussions.
- Use of personal email to communicate with or about any students.
- Introducing any form of malicious software onto the school network.
- To disrupt the work of other users, for example, includes the propagation of computer viruses.

#### **4g) Use of Mobile Phones and Personal Devices**

Under no circumstances should staff use their own personal device to contact students or parents/carers either in or out of working hours, unless with the express consent of the Headteacher and in these circumstances, the withheld number function must be used.

Staff are not permitted to take photos or videos of students on personal devices. If photos or videos are being taken as part of the school curriculum or for a professional capacity school equipment must be used.

Staff should not use their phone in class, in lessons, on corridor, on duty or whilst supervising students. Staff use should reflect the invisible policy of the school. This means staff should have their phones on silent and hidden whilst with students. Staff can use their phones at unstructured, free times and within privacy of offices or staff room. Staff should use school mobile phones for trips and residentials and these can be used at all times for the trip.

Any device which takes images, videos, moving images should not be used during working time as this unless it is specifically agreed by the Headteacher and the device is used for work purpose that do not involve video, images or photographs. Members of Staff who are Session Manager will use a school phone to access the Class Charts App only. These phones are school property and will only be used for this function. Staff will sign a document with regulations when they are assigned such a phone.

The use of personal equipment within the school can only be authorised by the Headteacher or Senior Leadership Team member in order to comply with Safer Working Practice guidance, General Data Protection Regulations and school policies related to safeguarding.

Any breach of the Online Policy may result in disciplinary action against that member of staff.

#### **4h) Inappropriate material**

In law there is a distinct difference between material that is inappropriate and that which is illegal, however accessing of inappropriate material is a significant concern with regards to safeguarding and staff conduct and can lead to disciplinary action. Staff should be aware that the accessing of illegal material will lead to a police investigation, allegations management procedures, a possible criminal investigation, prosecution and barring, even if there is no criminal prosecution.

#### **4i) Illegal material**

It is illegal to make, possess or distribute indecent images of a person under the age of 18 and viewing these images online may constitute possession of these images even if they are not saved. Accessing indecent images, real or doctored, of children or students on the internet or making, storing or distributing such images of students or children is illegal and if proven could lead to criminal investigation and the individual being barred from working with children.

#### **4j) Illegal incidents**

If there are any suspected illegal materials or activities found or suspected, the school will report it immediately to the Police, and report under local safeguarding arrangements.

## Appendix 5      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, Safeguarding and Positive Behaviour Policies.
- 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 and to protect these.
  - 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.
  - Not to contact staff on social media, search for staff, friend request or make images of staff or comments about staff on social media
  - Not to contact peers on social media, without consent, to harass or abuse. To coerce or pressure friend requests or make images of peers or comments about peers on social media
  - To not post images of peers online wearing uniform or to disclose school or personal information about peers online
  - To not post or share, comment, or 'like' negative content or contact about a peer or other adult
  - To adhere to the schools zero tolerance approach to all forms of bullying online and offline
  - To use etiquette and manners in all forms of online communication including school and personal communication
  - Be aware of their own digital footprint
  - Be responsible for managing social media posts and gaming with strangers safely
  - Understand that school will and can sanction for poor online behaviour that occurs out of school

## **Appendix 6: Student - Use of Personal Mobile Phones**

At Horsforth School we recognise the widespread ownership of mobile phones amongst our young people and the increasing dependence by all, on new technologies. However, we also know that the possession and use of mobile phones can be highly disruptive to learning, whilst also posing a threat to our safeguarding procedures. This does mean as a school we need to ensure that mobile phones are used responsibly. These procedures are designed to limit the disruption and potential issues involving mobile phones, whilst ensuring that the benefits that mobile phones provide (such as increased safety) can continue to be enjoyed by our students.

These procedures have been developed taking into account parental consultation on the use of phones.

Horsforth School accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. It is evident that there is concern about students travelling alone on public transport or on their journey to and from school.

The School acknowledges that providing students with mobile phones for school, gives parents /carers reassurance as that they can contact their child if, on their journey should there be an emergency.

**To this end, the following will apply:**

### **Responsibility:**

Parents/carers should be aware if their child is bringing a mobile phone, the child is responsible for the phone and that they must abide by the guidelines of these procedures. Please note the school is not responsible for the phone and that the phone is brought into school at the owners' risk. School does not accept responsibility for mobile phones and school is not liable for lost, broken or stolen phones. It is assumed that parents/carers have insurance for the phone.

## Procedures:

- Students may bring mobile phones to Horsforth School for use on **the way to and from school only**.
- Phones and electronic devices must **not be visible, heard or used at any time**, on the school site, during the school day (**8AM-4PM**). **They must be switched off at all times and in bags. Students should not therefore be able to access the internet on their own 4G/5G plans unsupervised.** This includes: before and after school starts/finishes, break time, lunch time, all lessons, lesson changeover, corridors, or on the external site (tennis courts, yard, toilets, courtyards, Astro-turf, playing field, benches, front and back paths leading to and from the main building).
- This also includes all electronic devices: MP3 players, iPods, Air Pods
- Phones and electronic devices should be **switched off** and stored securely in **school bags only**. This needs to be done before students enter the school grounds.
- Phones and electronic devices should not be visible; therefore, students are not permitted to store them on their person, in pockets or in coats. Phones seen in pockets or on the person will be deemed visible and confiscated.
- Phones that sound or that are turned on (even within bags) will be in breach of this policy and confiscated.

## Confiscation:

**Any visible electronic device or phone that is visible (whether it is being used or not) on school site and during the school day will be confiscated and sanctions will be issued.**

## Sixth Form

Students in years 12 and 13 are permitted to use their phones in their free time, in common rooms, in designated areas outside by common grounds and social areas in the sixth form block only. This is for work related learning. Teachers may allow phone use for work related learning in class at their own discretion.

Students must use their phones responsibly and will be subject to sanctions, and a confiscation if they are not. Students are reminded of these rules at induction and in the year.

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.

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 and Staff Disciplinary.

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.

**Whilst onsite year 12 and 13 pupils may use the school Guest Wi-Fi on their personal devices (phones) in order to help them carry out their studies. To use the Guest Wi-Fi students should, find the broadcasting Guest Wi-Fi and connect to it. Once connected they should open up a webpage, they will be challenged by the web filtering portal where they should only enter their own school username and password.**

**Whilst onsite students must switch off and not use any private data plan. Students must also turn off any hotspots on their devices to prevent sharing of connections as they will be responsible for any activity associated with their login.**

#### **6a) 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.
- Phones are protected by a security code and kept locked.

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 other personal device or have committed a criminal offence, the police will be contacted.

## **Appendix 7a: 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. (see Appendix 7b).

All members of the community must use the official school procedures for reporting concerns through CPOMs and/or SIMs for Behaviour procedures. (see flow chart, Appendix 7b).

The school requires staff, parents, carers and students to work in partnership to resolve online safety issues.

After any investigations are completed, the Child Protection 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 Education Safeguarding Team.

Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm. Other Safeguarding Partners maybe contacted at this point.

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.

### **Typical Online Incidents**

Typical online incidents perpetrated by pupils, staff, parents, Trustees, contractors and others could include:

- Finding illegal material on the network which could raise a child protection issue.
- Going on the Internet during lesson time for reasons not related to the lesson.
- Bypassing the school's filtering system.
- Viewing pornographic material.
- Using a mobile phone or other digital device in a lesson.
- Using social media or email during a lesson.
- Cyber bullying.
- Writing malicious comments about the school or bringing the school name into disrepute (whether in school time or not).
- Sharing usernames and passwords.
- Deleting someone else's work or unauthorised deletion of school files.
- Attempting/gaining unauthorised access to another person's account(s), electronic services and data provided by the school.
- Uploading or downloading files using school accounts, devices or services which are illegal, inappropriate or puts services at risk.
- Copyright infringement of text, software or media.

SurfProtect Quantum+ alerts designated staff of any inappropriate searches carried out by staff and pupils by way of instant alert emails and a daily digest email report. These reports are checked by designated staff and where further investigation is required, they are escalated in the first instance to the Behaviour Support Team or DSL(staff).

The school's approach to dealing with an incident and applying sanctions aims to demonstrate the correlation between procedures and sanctions for pupils and procedures and sanctions for staff.

The reporting process and sanctions will depend on:

- Whether an illegal act has taken place
- Whether there is a safeguarding issue (in which case we will follow the guidelines in our Safeguarding and Child Protection Policy)
- Whether the issue is low level and can be dealt with by internal procedures
- The nature and severity of the incident
- Whether the incident is a form of bullying
- Whether the incident is in or out of school
- Whether there has been a serious breach of the Positive Behaviour Policy
- Whether the person has previously had sanctions for a similar incident

Note that under The Education and Inspections Act 2006 Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they breach the school policy.

These general principles apply in dealing with an incident of Safeguarding:

- The DSL/DSO or SLT will collate and secure any – this may involve assistance from the schools IT Support Team and/or external IT contractor(s). Images will not be viewed unless the DSL has good reason to do so. The DSL must be consulted. The DSL will seek further advice.
- Incident reports will be completed and submitted to DSL via CPOM's and in person if urgent. Depending on the nature of the incident it should also be logged on SIMs.
- Appropriate disciplinary action/sanctions/ support will be taken following the school's procedures and/or external advice.
- Parents/carers may be informed.
- The police and/or other relevant agencies such as PREVENT will be notified in certain circumstances, including:
  - if an indecent image has been taken – sexting
  - in the case of cyberbullying or hate crime
  - harmful sexual behaviour
  - extremism, fundamentalist ideologies / materials
  - an incident of hacking or online fraud
  - any crime where child is considered a victim or abuse or exploitation

### **8a) 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.

### **8b) Dealing with 'Sexting'**

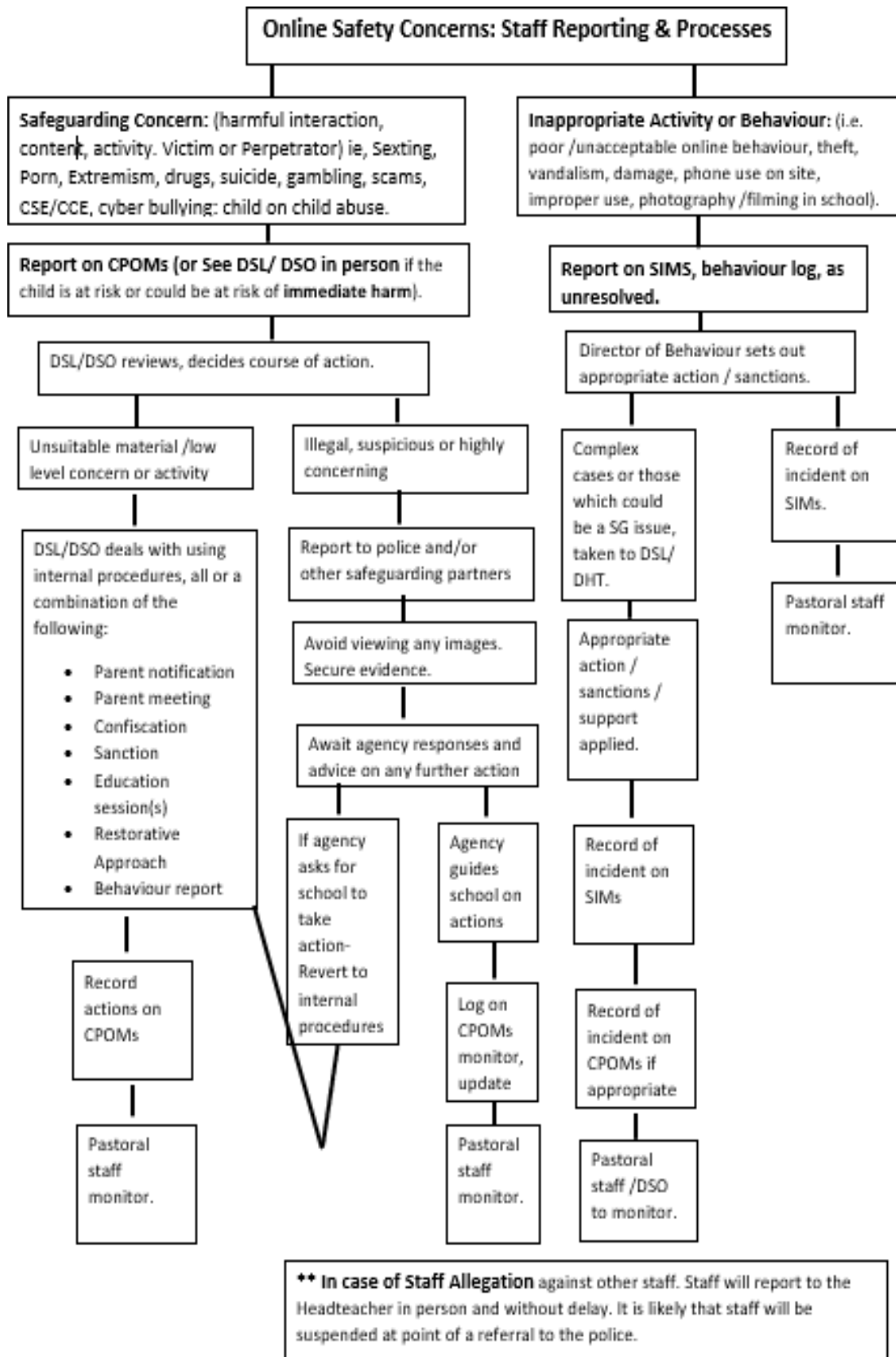
If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:

- 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.
- 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.

## Appendix 7b: Reporting Online Safety Incidents and Concerns



## **Appendix 8: Procedures for Responding to Specific Online Incidents or Concerns**

### **8c) Online Child Exploitation**

- We will ensure that all members of the school community are aware of online child sexual abuse and online child criminal exploitation including grooming; signs and indicators, the consequences; possible approaches which may be employed by offenders to target children and how to respond to and report concerns.
- We recognise online child exploitation as a serious 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 abuse and exploitation 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 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.

### **8d) Dealing with Online Child Abuse and Exploitation**

- If the school are made aware of incident involving online abuse and exploitation 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 (Child Exploitation Matrix Tool) 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 Children's Social Work 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 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.

### **8e) 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, Children's Social Care, or the LADO for staff.
- 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](http://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 Police and 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.

## 8f) Cyberbullying

Cyber-bullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites. Examples of cyberbullying include abusive text messages or emails, rumours sent by email or posted on social networking sites, and distributing embarrassing pictures, videos, websites or fake profiles.

- Cyber-bullying by students and staff will not be tolerated and will be treated as seriously as any other type of bullying. Information about specific strategies or programs in place to prevent and tackle bullying can be found in the Anti-bullying Policy.
- If a member of staff is aware of a bullying incident they must take this seriously, act as quickly as possible to establish the facts and report the incident to the appropriate member of staff via SIMS, CPOM's or in person.
- These members of staff will investigate the matter fully, provide support for the victim, and alleged perpetrator (as appropriate) to act restoratively and apply sanctions when necessary.

- If a sanction is used, it will correlate to the seriousness of the incident and the bully will be told why it is being used. The student will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it.
- Any allegations of cyber-bullying by students will be managed in accordance with the Anti-bullying Policy and Positive Behaviour Policies.

### **8g) 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.

### **8h) 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.
- The DSL will liaise with the PREVENT team in Leeds. A referral may be made after the initial call and advice from this.
- 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.

### **8i) Harmful Sexual Behaviour, including Child on Child Abuse**

- We recognise that children do abuse children online. This includes sexting, online sexual harassment, online threats or blackmail. 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 /or the AIM guidance and checklist for Harmful Sexual behaviour.
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of harmful sexual behaviour and child on child abuse by implementing preventative approaches, via a range of age and ability appropriate educational methods.

### **8j) Dealing with Online Harmful Sexual Behaviour**

The DSL will use the AIM guidance and checklist to judge what action needs to be taken. The school will:

- Act in accordance with our Child protection and Safeguarding policies
- 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 Children Social Work Services and/or the Police.
- 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.**

## **Appendix 9 Confidentiality and Data**

Members of staff have varying degrees of access to confidential information or data about students, other staff and parents/carers in order to undertake their daily duties, this may sometimes include highly sensitive information. This information must not be shared outside of the school or with external parties unless there is good reason to do so, for example a student is at risk of harm or significant harm, there is an agreed multi-agency plan around a family or student, a behaviour managed move or for attendance interventions, which means that sharing of information is in the best interests of the student.

Confidential information should only be stored on school systems and devices. Emails should not give full details of a student. Confidential information will be only transferred in email if it is password encrypted. Staff should consult with HR if they are unsure.

Any data handled or stored by school done so in accordance with the GDPR and Data Security Policy. The storing and processing of personal information is governed by the General Data Protection Regulation and Data Protection Act 2018. Employers are required to provide clear advice to staff about their responsibilities under this legislation so that, when considering sharing confidential information, the principals set out in this legislation apply.

For further information in relation to confidentiality issues and safe storage of data please refer to the Safer Working Practice Guidance.

## **Appendix 10: Equal Opportunities**

The school believes that it is essential that everyone can have access to ICT when working from home and that learning opportunities should be provided for all students, regardless of their ability, ethnicity, age, gender, sex, gender identity, beliefs, values, religion, culture and whether they have a Special Educational Need and/or Disability (SEND).

This is underpinned by the requirements set out in the Equalities Act 2010.

ICT can be a positive tool for students with SEND and access to the internet and ICT can be a vital link for communication with the outside world, which can enable every student to have access to information, communicate with others and develop ideas and research independently.

## **Appendix I Ia: 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.
- 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. That, 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, such as for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- That it may be a criminal offence or breach of Horsforth School policies and procedures to download or share inappropriate, harmful pictures, videos or 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 and 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.
- 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.
- Will not take or distribute images of anyone without their permission
- 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 not use social media sites at school or use my phone whilst on school site.
- I will use social media sites responsibly out of school so as to not cause harm, risk, distress or danger to any member of the school community

**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 do not follow with this Acceptable Use Agreement, I could be sanctioned. 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 or devices is governed by the Online Safety Procedures and all of the policies and procedures available from Horsforth School’s website [www.horsforthschool.org](http://www.horsforthschool.org) when:**

- I use Horsforth School systems and devices (both in and out of school).
- 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. mobile phones, social media, 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 I Ib: 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.
- 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 follow the school's policy for use of AI.
- 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 DSL/ 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 I2: Safeguarding for Remote Learning**

### **9.1 Rationale**

Keeping both students and teachers safe when providing remote education is essential. Remote education has been and can be a new experience for both staff and students, so it is important that everyone understands how to approach safeguarding procedures online.

### **9.2 Objectives and Suitability**

Lesson objectives should be carefully considered and the most appropriate technology selected for the task. This should include a consideration of the age and ability of the students and the number of students. Many students feel they benefit from regular real-time interaction to supplement other learning activities.

### **9.3 Timing of Communication**

As always, staff should not communicate with parents or students outside school channels (e.g. they shouldn't talk to parents using their personal Facebook accounts, or contact students using their personal email addresses or phone numbers). There is an expectation that the majority of communication with students will be during normal working hours.

### **9.4 Personal Data**

It is important to take care not to share personal data (e.g. email addresses). Make use of the BCC function wherever possible, including for groups of students. It is good practice when emailing a group to email yourself and put all recipients as BCC. Staff should take care to handle the information and data relating specifically to students, for example, they should not circulate lists of students yet to complete work.

### **9.5 Communication with Parents / Carers re remote learning**

Parents / carers will receive regular reminders about online safety and our behaviour/etiquette expectations. This advice will include setting appropriate security settings, reporting online bullying or abuse and ensuring that any online tuition is organised and appropriate and supervised carefully. Students will be sanctioned for poor and unacceptable behaviour.

### **9.6 Safeguarding**

Any safeguarding incidents or potential concerns should be passed to the DSL in the usual way. Any cause for concern regarding the child's safety or wellbeing should be reported. This would include possibly abusive behaviour by the parents or other family members, indications of self-harm or bruising, or change in mood or behaviour of the child in question. The safeguarding policies remain the same regardless of the location of potential danger or abuse. All concerns regarding a student's wellbeing should always be reported to the DSL immediately. All staff have access to CPOMs remotely and can phone the DSL direct out of hours. The DSL will explore the issue and follow the school safeguarding procedures.

### **9.7 Choosing an appropriate platform, service or app**

Platform's must be approved and regulated by the school, otherwise, staff put themselves and others at risk. We use Google Classroom and Microsoft 365/Teams, these are the safest platform and easiest as it sits within the school's Microsoft and Google package.

### **9.8 Appropriate Access and Behaviour for Online Learning**

Always schedule a meeting in advance and end the meeting prior to leaving, ensuring that students cannot be left in a meeting.

Never publicise a meeting on social media.

By using “meeting options” when setting up your meeting, you can set who can bypass the lobby, to “only me” – this will allow you to control who has access and when to the meeting. Teachers should make clear their expectations at the start of any interactive sessions. These should be as close to a ‘classroom standard’ as possible.

One particular issue is the protocol for who may speak and when. If this is the first time that classes are delivered online, it may take some time in becoming familiar with the new environment. Make sure that all conversations are: (a) Necessary for the student’s academic development (b) Not involving too personal information (c) Not taking up much more time than you would if you were physically at school (d) Not outside of school hours.

To talk to a student online individually as a Tutor or for pastoral care, ensure this is planned and that it is part of a guided instruction from SLT or DSL. Record the conversation as protection.

### **9.9 Location/Environment**

When making recordings or undertaking interactive sessions There should be careful consideration of the location that everyone uses. Staff should be mindful of their setting when recording broadcasts or taking part in interactive sessions. Pick a neutral area of your home when on video. Make sure to always be wearing appropriate clothing when on camera. Once you’ve chosen the appropriate spot to be on camera, think about what’s in the background. You can change the background to remove any views of your home and replace it with a scenic picture or neutral colour.

Young people should also be in an appropriate location within their home – consider what can be seen and heard and whether this is appropriate. We use Google Classroom and Teams as they allow the teacher to disable users’ microphone and video cameras. Staff should ensure that you are familiar with how to operate these functions before you start any interactive sessions.

### **9.10 Recording and sharing**

When undertaking remote sessions, teachers should make a note of the conference timing and record sessions.

They should use MINT seating planner to mark present those that participated. MINT will update SIMs registers held centrally within school. School can therefore track attendance for a range of issues including safeguarding.

It is not acceptable for students to record events.

If the service records the conference, make sure that everyone is aware of this.

### **9.11 Personal Data**

Staff and students should only use school-provided email addresses and create appropriate usernames (if necessary). Livestreaming Lessons Livestreaming is transmitting or receiving live video and audio coverage of an event or person over the Internet. When livestreaming face to face lessons to students who are self-isolating at home, teachers must take care to ensure that the camera is focused on the teacher or the board, not the students in class. Ensure that students are aware that the lesson is being live-streamed to other students outside the classroom.

### **9.12 Recording Segments of Lessons**

If you decide to record a segment of a lesson to be shared later with students, for example, an experiment or an explanation, it is vital that other students are not captured on this.

### **9.13 Use of personal mobile devices Personal mobile phones**

For years 7-11, these must not be used in lessons for any school work purpose.

In sixth form students may be allowed to use phones for work purposes at the discretion of the teacher, e.g. photos of classwork, video of practical work.

For all year groups, they may not be used to photograph students/staff or video students/staff.


## Appendix 13: ICT Staff 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 from 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.
- 5.8 **One Drive.** You can use Microsoft One Drive as a personal storage space (it currently limited 30GB) to save school work which can be accessed anywhere in the world. The OneDrive is backed up by the school periodically.

## 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 \_\_\_\_\_

## Appendix 15 Filtering and Monitoring Procedures

### Summary of the Filtering and Monitoring Systems we use at Horsforth School - SurfProtect Quantum+

EXA Networks provides a secure, filtered and monitored internet service for the school. EXA Networks utilises the SurfProtect Quantum+ filtering system to check and record all internet traffic ensuring it meets Ofsted compliance and Prevent Duty legislation. EXA Networks are approved by the government and the Internet Watch Foundation for use in schools.

All traffic is logged and stored away from the school. School staff do not have the ability to modify or delete logs thus ensuring integrity of the data for audit and legal purposes.

Every pupil and member of staff has a unique login on the SurfProtect Quantum+ platform (which runs silently in the background when they use a school computer or laptop). Each account has filtering applied based on the users age/role.

If pupils bring in their own devices (BYOD) and use the schools BYOD Wi-Fi connection. They will be challenged by the SurfProtect Quantum+ platform to enter their username and password, after successful login they are granted the same level of web filtering as they would on a school device.

Instant email alerts are emailed to the IT Services Department which shows any activity which may have been deemed inappropriate (this activity would have been denied but logged). These alerts are reviewed and the following action taken:

For Pupils: Activity warranting further investigation is logged onto CPOM's for follow up by the Safeguarding Team.

For Staff: Activity warranting further investigation is reported to the HR Director and/or Designated Safeguarding Lead for further review.

Should a site that has been blocked require unblocking then IT Services will only accept the request via email (for record purposes). The site is then reviewed and if deemed suitable for use in school then the IT Services department will either grant access to the site by modifying the filtering rules or refer it back to EXA Networks for them to action the modification of the filtering rules.

The filtering system is checked daily to ensure it is working. Once a month a further independent check is performed using a site called Test Filtering to confirm the web filtering is working to DfES standards independently of the EXA Networks and SurfProtect Quantum+ .

The DSL, LT and Trustee will make checks ad hoc through the year, these are recorded in the annual online safety report.

What is blocked, filtered and monitored is reviewed annually.

1 <https://exa.net.uk>

2 <http://testfiltering.com>

### Roles and Responsibilities:

Clear roles and responsibilities are vital for the delivery and monitoring of effective systems. At Horsforth we ensure the right people and teams are working together on filtering and monitoring so we utilise the range of professional expertise.

## **The DSL:**

The DSL has ultimate responsibility and oversight for all aspects of online safety including filtering and monitoring. The DSL is closely supported by the Headteacher, the IT services lead and team, Curriculum Leaders for PSHCE, ICT and computing, Director of HR and the lead safeguarding Trustee.

The DSL and Trustee ensure that standards and legislation are met.

- The DSL will ensure online safety is in embedded curriculum.
- The DSL will ensure staff have relevant and frequent training as part of safeguarding training and specifically on filtering and monitoring.
- The DSL will ensure parents and carers are provided with online safety updates via letters and on the website.
- The DSL will act on reports and concerns and take relevant action.
- Oversee the acceptable use agreement with all stakeholders.
- Oversee quality assurance of filtering and monitoring.
- Will work closely with IT services and lead the online safety group.
- Will oversee the annual online safety report.
- Review effectiveness of filtering and monitoring systems.
- Make the decision as to what the school blocks or is allowed annually or at key times as they arise.
- Work closely with lead Trustee for safeguarding whose role includes oversight of filtering and monitoring.

## **IT Services Lead:**

The IT services Lead will procure the right filtering and monitoring system for the school.

- Will be the day to lead and overall manager for the filtering and monitoring systems in school.
- Ensure efficacy throughout the year, complete monthly checks and ensure compliance.
- Will be intrinsic in the annual review, complete the online safety report, produce data and attend online safety meetings.
- Oversee daily reports from SurfProtect Quantum+.
- Ensure concerns are given to the DSL or HR in a timely manner and to know what to do if the concern is urgent.
- Work within relevant guidelines.
- Assist on concerns, support action/ investigation.
- Lead on training for filtering and monitoring for all stakeholders.
- Support the lead Trustee and meet with lead Trustee
- Support staff with queries and concerns.

## **Online Safety Group:**

Meet once per half term to monitor, check and review all aspects of online safety including filtering and Monitoring. The Lead Trustee will attend where possible, but will be updated on minutes/ actions.

- The DSL
- DDSL's
- IT Services
- PSHCE lead
- ICT and computing leads

## **All Staff**

- Will comply with the acceptable use agreement for their own devices and school devices.
- Will be vigilant with use of ICT in the classroom and ensure clear objectives for the use of ICT.
- Will check websites and prepare ICT work in advance so as to consider 'safe' content and the schools filtering and monitoring systems.
- Use every opportunity when using ICT as a resource to remind students about acceptable and safe use.
- Know signs and indicators of abuse and exploitation online.
- Report concerns on CPOMs or see a DSO in person if urgent.
- Will complete cyber security training and online safety training which will include filtering and monitoring.

## Appendix 16 Use of Generative AI (Artificial Intelligence)

**\*This Appendix will be kept under review during 2025-2027 and will change subject to updates**

- Students do not use any form of AI in school as part of agreed learning 2025-26.
- Students are not allowed to use AI whilst in the building or on school devices.
- Students are not allowed to use any form of AI for any form assessment, formal or informal. Students will be sanctioned for plagiarism.
- The school uses approved filters to block the use of AI by students.
- Generative AI is for staff use only for 2025-26. The DfE (Generative artificial intelligence (AI) in education 2025) states 'there are more immediate benefits and fewer risks from teacher-facing use of generative AI only'.
- Staff must log in to AI using their school login/passwords whilst using AI for school purposes on or off site.
- Net Support Classroom cloud monitors all keyboard activity done on any device in school and this covers staff use of AI to ensure safe use. Through the school filtering and monitoring tools via Classroom Cloud it can track and capture any unsuitable word or content typed into generative AI which could be a safeguarding breach. An immediate alert is flagged with the safeguarding team for immediate action.
- School will ensure that a generative AI tool will be used only and that teachers will be asked to ensure correct standards for **accuracy, security, privacy, data protection, and child safety**, aligned with the DfE's expectations.
- The main generative AI tools used by staff for 2025-26 will be ChatGPT, Microsoft Copilot, Claude and Google Gemini. These can:

1. answer questions
2. complete written tasks, generate images, text or code
3. respond to prompts in a human-like way

- Generative AI could be used for:

creating educational resources  
lesson and curriculum planning  
tailored feedback and revision activities  
administrative tasks

- Staff will check and quality assure the content from generative AI as it could be:

inaccurate  
inappropriate  
biased  
taken out of context  
taken without permission (intellectual property infringement)  
out of date or unreliable  
low quality

- Teachers are asked to use their professional judgement when using these tools. Any content produced requires critical judgement to check for appropriateness and accuracy. The quality and content of any final documents remain the responsibility of the professional who produced it at the school regardless of the tools or resources used.
- Teachers will not input any personal, sensitive, or safeguarding data (e.g., pupil names, parent names, SEN details, SIMs, or CPOMs incidents) into AI.
- The schools working party for AI will review the use of AI and update these procedures in line with further guidance or the need for new parameters.