High Grange

***A**daptive thinking, **C**ommunication, **E**motional wellbeing, **I**ndependence*

Promoting Wellbeing & Safety		
Online Safety Policy		
Last Update: **September 2025**	Responsible: **Principal**	Page: **1 of 19**

This policy promotes ACE because;	
Adaptive Thinking Communication Skills Independence Emotional Wellbeing	**This policy promotes:** adaptive thinking through recognising online risks and using the Stop–Think–Check–Report routine; respectful communication and clear reporting routes; and emotional wellbeing by building resilience to cyberbullying, setting healthy boundaries, and knowing how to block, report and seek help while managing passwords, 2FA and digital footprints.

Contents

Contents:

1. Introduction
2. Legal Framework
3. Ethos/ACE
4. Aims
5. Approach
6. Roles and Responsibilities
7. Online Safety and the Curriculum
8. Use of Technology in the classroom
9. Use of Smart Technology
10. Educating Parents
11. Education and Training
12. Responding to Incidents of Misuse
13. Filtering and monitoring online activity

1. Introduction

In contemporary society, individuals across all age groups regularly interact with a variety of Internet-connected devices, such as smartphones, tablets, and smartwatches. These interactions provide numerous advantages, including enhanced communication, learning opportunities, and social engagement. However, they also expose children, young people, and adults to potential risks.

High Grange School is committed to promoting online safety for all members of our school community, encompassing children, young people, and adults alike. This commitment involves providing education on the risks and responsibilities associated with Internet and electronic communication usage, both within and beyond the school environment. This is an integral component of our duty of care to safeguard all individuals associated with our institution. We also prioritise the safety of our staff and foster robust digital literacy skills among our pupils.

Recognising the dynamic nature of technology and its usage patterns, our policies for safe Internet and technology use are continuously updated to remain current. We acknowledge the need for ongoing training and education in online safety, and, accordingly, all staff receive mandatory annual training. This training includes updates on emerging technologies and apps and is delivered by an in-house CEOP Ambassador. This approach ensures that our staff are well-informed about evolving online risks and maintain a direct link to CEOP's resources. On occasion, we may engage external experts to further enhance our knowledge.

High Grange School incorporates online safety into its curriculum across all age groups and employs interactive displays to raise awareness of potential online risks and hazards. We acknowledge that new technologies are an integral part of the lives of our pupils, both within and beyond the school setting. These digital tools offer numerous educational opportunities, promoting discussion, creativity, and context awareness to enhance effective learning and foster positive digital well-being.

We believe that all our pupils and young people are entitled to engage in the online world safely and confidently. Therefore, ensuring their appropriate and secure use of the Internet and related technologies is a fundamental aspect of our broader duty of care to the school community.

2. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Department for Education (DfE) — Keeping children safe in education (KCSIE) 2025
- DfE — Behaviour in schools (19 February 2024)
- DfE — Use of reasonable force in schools (updated 15 January 2025)
- DfE — Searching, screening and confiscation (updated 19 July 2023)

- DfE — Teaching online safety in schools (12 January 2023)
- DfE — Filtering and monitoring standards for schools and colleges (current page)
- DfE — Mobile phones in schools (19 February 2024)
- UKCIS — Sharing nudes and semi-nudes: advice for education settings (11 March 2024)
- UKCIS — Education for a Connected World (2020 edition, current)
- Working Together to Safeguard Children (December 2023)
- National Cyber Security Centre — Small Business Guide: Cyber Security (current page)

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Empowering resilience through ACE
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy

3. Ethos/ACE in Online Safety

Our School Ethos reflects our core beliefs and vision, guiding our holistic child-centred approach to education and development. It is encapsulated in our ACE Ethos, comprising three key elements cantered around promoting independence. The ACE Ethos is the cornerstone of all learning and experiences at High Grange School.

In the course of their daily lives, our pupils encounter the online world. The ACE Ethos equips them with the necessary tools to navigate this digital realm safely and effectively. By practicing these skills, pupils develop independence in an ever-evolving online environment.

Our School's Ethos is integral to our overall success, serving as the foundation of our philosophy and driving everything we do. It was meticulously crafted with input from our entire staff team, with a specific focus on the needs of pupils with Autism (ASC). Our new Ethos provides all pupils with a solid platform to enhance their daily experiences, preparing them for greater independence. The key areas of adaptive thinking, communication, and emotional well-being converge to ensure that all our pupils leave High Grange School equipped with the skills and attributes necessary for leading happy, enriched lives within the community, as independently as possible.

Online safety is a priority for all our pupils, and they are offered opportunities to develop their personal skills in adaptive thinking, communication, and emotional well-being. These opportunities are integrated into our specialised environment across all subjects, with a particular emphasis on PSHE, Citizenship, and Computing lessons. Pupils with ASC receive tailored information tailored to their specific needs, delivered with the necessary time, patience, and care to ensure a comprehensive understanding of online risks. They are provided with the space and support needed to process this information and to engage in discussions and formulate positive strategies for addressing concerns or dangers online. This approach not only equips them with an understanding of the digital world but also fosters a positive digital well-being as they transition towards greater independence.

This approach offers all our pupils the chance to achieve, grow, and develop the skills required for living as independently as possible. It empowers them to make informed life choices, ultimately leading to enriched and contented lives.

4. Aims

The purpose of this policy is to establish the ground rules we have in school for using computing equipment, smart technologies and the Internet.

This online policy will help to ensure safe and appropriate use within High Grange and enable them to be safe and appropriate independently also. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies and applications can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge. (i.e. upskirting, sharing nudes and semi-nudes)
- Power imbalance to coerce, manipulate or deceive younger people into criminal or sexual activities.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying. (As well as other forms of online harassment such as cyberstalking, doxing, trolling, hacking, threats, revenge porn, online impersonation, etc.)
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person and their overall mental health.

Many of these risks reflect situations in the off-line world and it is essential that this online policy is read and used in conjunction with other school policies; specifically Anti-Bullying, staff acceptable usage, Behaviour, Safeguarding/Child Protection and Mobile Phone and technology Use.

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

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The online policy explains how the school intends to do this, whilst also addressing wider educational issues to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communication technologies for educational, personal and recreational use.

5. Approach

High Grange School delivers online safety through the following categories:

- Education:
- High Grange School delivers education as part of the curriculum in Key Stage 1, 2, 3, 4 and 5.
- Online safety is targeted across all curriculum areas through pupils being closely monitored and keeping pupils safe on the internet whilst in school. High Grange School ensures where possible that inappropriate websites are blocked and that access to inappropriate websites and material are restricted. Staff encourage and monitor pupils carefully to ensure that pupil safety on the internet is of paramount importance.
- Online safety in terms of educating pupils is covered formally in pupils computing lessons, PSHE lessons and Citizenship lessons across all age groups, tailoring the level of depth around the subject to different age groups, as well as the individual. This includes the opportunity to complete the BCS 'Smart Digital' qualification in Key Stage 4 core lessons. This is an accredited level 1 qualification with a strong focus on online safety.
- Information on online in terms of guidance and keeping children safe whilst accessing technology at home is also sent to parents/carers from school.
- High Grange school aims to update parents/carers with the most up to date information as much as possible, through the website, letters and leaflets being sent home, face to face meetings and 'coffee mornings'.
- High Grange School gives pupils opportunities outside of standard lessons to engage in learning about online safety, such as during Online Safety Week which is held annually. This is organised across various year groups through the entire week.

- Web Filtering - High Grange School uses Barracuda web filtering service to ensure pupils only access websites that are appropriate for them. This is updated regularly by both the Barracuda web filtering service and by IT staff in school. It is customisable to the point where each pupil can have their individual restrictions placed upon their use of the internet.
- Staff Support - All staff at High Grange School have annual mandatory training in online safety; Staff support to pupils using technology is vital to online safety. Staff within High Grange have a duty of care and must have read and comply with High Grange safeguarding policy. This ensures that any individual concerns are raised.
- Contact with Families - High Grange School recognises the need for excellent communication links with the families of pupils within accessing the school setting. The school has a designated home liaison officer to ensure that parents/carers have a consistent route to contact the school but are also updated on changes within the school that may affect the pupil. This contact is key to developing online support at home.
- Newsletters – High Grange School through support from our Pastoral lead, create Newsletters that are sent home to parents that identify current trends and topical issues with support for parents.

6. Roles and Responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensure the school uses a firewall and robust antivirus software
- Ensure the school uses a recognised internet service provider
- Ensure the school uses an encrypted and password protected WiFi network
- Receive a termly DSL report on online-safety incidents, trends, and filtering/monitoring effectiveness.
- Ensure the review cycle remains annual or sooner if guidance changes.

The Principal and Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the DDSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training. HGS have internal online safety training annually from ~~Nathan Barrington~~ High Grange CEOP ambassador. External training annually from ~~Tracie Wild~~ parent governor.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and HGS IT support to conduct half termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

The DSL has lead responsibility for online safety. All staff receive safeguarding training, including online safety and filtering/monitoring awareness, at induction and updated regularly; records of staff completion are maintained.

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the schools IT support and safeguarding leads.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the Headteacher and governing board to update this policy on an annual basis.

Online CEOP Ambassador – This role is currently held by Nathan Barrington that receives regular training and then shares this between the teachers safeguarding officers and pastoral staff, as well as Rushcliffe care IT support staff. The responsibilities are as follows:

- The school's ICT infrastructure is secure and meets online technical requirements
- The school's password policy is adhered to.
- The school's filtering policy is applied and updated on a regular basis – this includes updates to DDSL.
- To keep up to date with online technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail etc.) is regularly monitored so that any misuse or attempted misuse can be reported to the Online Coordinator and/or SLT for investigation
- 1:1 education with pupils when appropriate or needed.
- Discussion regarding online issues with pupils.
- Debriefing with pupils.
- Explaining to pupils why they may be in danger.
- Creating toolkits for parents to support the pupils as much as possible.

Designated Safeguarding Lead - Principal is responsible for managing the safeguarding/child protection team within the school.

Other staff who have safeguarding responsibility include:

- Designated Safeguarding Lead: (DSL) – Education: School Principal
- Deputy Designated Safeguarding Lead - Deputy Head teacher
- Safeguarding Leads

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online matters and of the current school online policy and practices
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- Online issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school's online and acceptable usage policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- They report any concerns they have about any pupil's use of technologies or apps that could endanger them or others.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Pupils (to an age-appropriate level):

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given

access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's online policy also covers their actions out of school, if related to their membership of the school.

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

- Endorsing (by signature) the Pupil Acceptable Usage Policy
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

7. Online safety and the curriculum

Our curriculum is mapped to Teaching online safety in schools (2023) and the UKCIS Education for a Connected World framework (current edition).

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE / RSE
- Citizenship
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in the PSHE and RSE subject policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

8. Use of Technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers / Desktops
- Laptops
- Tablets / Chromebooks
- iPads
- Kindles
- Interactive white boards

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

9. Use of Smart Technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Our approach to pupils' mobile phones is implemented in line with DfE Mobile phones in schools (2024) and our mobile phone & Behaviour Policy; breaches attract proportionate, consistent sanctions.

Pupils will be educated on the acceptable and appropriate use of personal devices including mobile phones and will use technology in line with the school's policies and procedures.

Staff will use all smart technology and personal technology in line with the school's code of conduct.

Pupils do not have access to the school Wi-Fi. Personal 3G/4G/5G data can bypass filtering, so use of personal devices is restricted during the school day. Any breach of this policy or attempts to access inappropriate content will be addressed through the mobile phone policy and, where relevant, the Searching, Screening and Confiscation guidance.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils are permitted to use smart devices in the classroom but they are closely monitored by staff to ensure when they are used pupils are on task and using their smart device to enhance their knowledge and skills within that particular subject area.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will take the appropriate action that may include removing the pupils personal mobile phone and enforcing a mobile phone ban in partnership with parents / carers.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

10. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will have copies of HGS mobile phone rules.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.

- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. ~~sexting~~ sharing nudes and semi-nudes.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Parent training / coffee mornings
- Termly newsletters that include safeguarding online information written by the schools Head of Pastoral care (Parent corner section)
- School website
- Information sent home with advice.

11. Education and Training

Online education will be provided in the following ways:

- A planned online programme is provided throughout the school's curriculum weaving the topic through various subjects. Online safety is regularly revisited in especially in computing and PSHE curriculum – this programme covers both the use of computers, new technologies, smart and phone applications and the internet in school and outside of school.
- Pupils are taught in lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of the information, while ensuring what they find is appropriate.
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet, mobile devices, other smart technology and the internet both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Artificial intelligence (AI).

Artificial intelligence (AI). Staff may use AI tools in line with DfE guidance, exercising professional judgement and checking outputs for accuracy and bias. Any AI use that processes personal data must comply with UK GDPR and our privacy notices. Sources: DfE "Generative AI in education" (2023 position, updated 2025) and ICO note on AI & data protection in schools.

Copyright:

- Pupils to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

Staff Training:

- Senior team are to ensure that all staff are aware of the procedures that need to be followed in the event of an online incident taking place. This will be revisited and refreshed regularly through training delivered by the CEOP Ambassador or an outsourced professional.
- A planned programme of online training is available to all staff. An audit of the online training needs of all staff will be carried out regularly.
- All new staff receive online training as part of their induction programme, ensuring that they fully understand the school Online policy, Acceptable Usage and Child Protection Policies.

Email:

- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/carers/ pupils.

Mobile Phones:

- School mobile phones only should be used to contact parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices
- Staff should not be using personal mobile phones in school during working hours when in contact with children. (Only variation is when supporting an offsite educational visit – staff mobile phones can be used to phone the school or contact emergency services should the need arise.)
- Pupils should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

Social Networking Sites:

- Young people will not be allowed on social networking sites or applications at school; at home it is the parental responsibility, but parents/carers should be aware that it is

illegal for children under the age of 13 to be on certain social networking sites or applications.
- Staff should not access social networking sites or applications on school equipment in school or at home. Staff should access sites or applications using personal equipment.
- Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site application, blogs, vlogs or any other technology at any time.
- Pupils/Parents/carers should be aware the school will investigate misuse of social networking, application or other online issues if it impacts on the well-being of other pupils or stakeholders.
- If inappropriate comments are placed on social networking sites, applications or online in any way, about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- Pupils in the KS1, 2, 3, 4 and 5 curriculum will be taught about online safety on social networking sites, application and other online enable technology, as we accept some may use it outside of school.

Digital Images:

- The school record of parental permissions granted/not granted must be adhered to when taking images of our pupils. A list is available in the admin office.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal.
- Where permission is granted the images should be transferred to school storage systems (online school servers) and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.
- The status of a pupil's care order will be checked prior to permissions being granted for digital images.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and ~~face-book~~ Facebook & Instagram page which are used to inform, publicise school events and celebrate and share the achievement of pupils.

Removable Data Storage Devices:

- Only removable media should be used that is provided by the school.
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.
- Staff are to encrypt any removable media device in case this device is lost or stolen, so that any important information is not breached or stolen.
- Pupils should not bring their own removable data storage devices into school.

- Pupils should not be connecting any personal devices to school serves or Wi-fi without specific permission from the Principal or ICT coordinator.

Websites: In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are monitored very closely when working with younger pupils who may misinterpret information, and to ensure how information is searched is done in the safest way possible.
- All users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed. Pupils are also aware that all internet use at school is tracked and logged.
- The school only allows the Online Co-ordinator, ICT co-ordinator, IT Technical Support Staff and SLT to access the Internet logs.

Passwords:

Staff should:

- Not record passwords or encryption keys on paper or in an unprotected file
- Change passwords at least every 3 months
- Not use the same password on multiple systems or attempt to "synchronise" passwords across systems
- Not allow pupils to use school computers through their account

Pupils should:

- Only let school staff know their in-school passwords.
- Inform staff immediately if passwords are traced or forgotten. All staff are able to request a password reset through the IT support ticket system, accessed at rushcliffecare.co.uk/support.
- Not allow other pupils to freely access their school accounts.

Use of Own Equipment:

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Principal or ICT co-ordinator.
- Pupils should be aware that any personal devices are brought into school at their own risk.

Use of School Equipment:

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

- Staff should ensure any screens are locked (by pressing Windows and L keys simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring: All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the Rushcliffe care ICT support team and members of the Senior Leadership Team depending on the severity of the incident.

- The Rushcliffe care ICT support staff and ICT specialists within High Grange School will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the school who comes across an online issue does not investigate any further but immediately reports it to the online co-ordinator and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the Rushcliffe care ICT support staff, ICT specialists or CEOP Ambassador, then the member of staff should report the issue to the Principal).

Incident Reporting: Any online incidents must immediately be reported to the Principal (if a member of staff) or the ICT specialists or CEOP Ambassador (if a pupil) who will investigate further following online and safeguarding policies and guidance.

12. Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of computers and technology, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse.

If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Incidents involving sharing nudes or semi-nudes. Staff must not view, copy, share or ask a pupil to delete imagery. They must inform the DSL immediately, record the concern, and the DSL will follow UKCIS guidance, including risk assessment, containment, decisions on contacting parents/police, and support for pupils.

Where there are reasonable grounds, the school may search, screen and confiscate items, including examining data on devices, in accordance with DfE guidance. Any access to data, retention or deletion will be necessary and proportionate, recorded, and carried out by authorised staff with a witness. The DSL is informed the same day and safeguarding procedures followed.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

13. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and IT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. The DDSL will receive updates if any pupils attempts to access anything inappropriate online in the school day. Alerts will be sent to the DDSL and working with DSL and Head of Pastoral care will take the appropriate action for the pupil and inform parents / carers of anything that has caused concern.

Requests regarding making changes to the filtering system will be directed to the Deputy Head Teacher and DDSL. Prior to making any changes to the filtering system, IT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by IT technicians. Reports of inappropriate websites or materials will be made to the DDSL immediately via alerts, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL / DDSL and IT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined and each case will be taken into account on an individual basis. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

- Governors receive an annual written report on filtering/monitoring effectiveness, incidents and trends.
- A named senior leader and the DSL share oversight; IT manages technical operation.
- A documented risk assessment precedes any change to filtering; a change log is maintained.
- Balance protection with avoiding "over-blocking" that restricts teaching.