THE HARVEY GRAMMAR SCHOOL

Online Safety Policy

Approved: October 2021
Review Date: October 2026

Contents

Statement of Intent

The Harvey Grammar School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal Framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- Anti-Bullying Policy
- Behaviour Policy
- Managing Allegations Against Staff Policy
- Data Protection Policy
- Confidentiality Policy
- Curriculum Policies, such as: Computing, Personal Social and Health Education (PSHE), Relationship, Sex and Health Education (RSHE) and Citizenship
- Safeguarding and Child Protection Policy

- Staff Disciplinary Policy

Roles and Responsibilities

The Governing Body is 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 agreed schedule
- 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
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them

The Headteacher is 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 Deputy DSL / DCPC 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
- Ensuring online safety practices are audited and evaluated
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety
- 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 The Network Manager to conduct termly light-touch reviews of this policy
- Working with the DSL and Governing Body to update this policy according to the agreed schedule

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school
- Acting as the named point of contact within the school on all online safeguarding issues
- 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 SENCo and The Network Manager
- 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
- Ensuring appropriate referrals are made to external agencies, as required
- Keeping up-to-date with current research, legislation and online trends
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff

- Ensuring all members of the school community understand the reporting procedure
- 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 Body about online safety on an agreed schedule
- Working with the headteacher and The Network Managers to conduct termly light-touch reviews of this policy
- Working with the Headteacher and Governing Body to update this policy according to the agreed schedule

The Network Manager is responsible for:

- Providing technical support in the development and implementation of the school's Online Safety Policy and procedures
- Implementing appropriate security measures as directed by the Headteacher
- Ensuring that the school's filtering and monitoring systems are updated as appropriate
- Working with the DSL and Headteacher to conduct regular light-touch reviews of this policy

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to
- Modelling good online behaviours
- Maintaining a professional level of conduct in their personal use of technology
- Having an awareness of online safety issues
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online
- Reporting concerns in line with the school's reporting procedure
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Pupils are responsible for:

- Adhering to the relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online
- Reporting online safety incidents and concerns in line with the procedures within this policy

Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from the Network Manager and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online Safety is integrated into learning throughout the curriculum

- Online Safety Awareness is embedded in to the PSHE, RSHE and Assembly programme

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Disciplinary Policy. If the concern is about the Headteacher, it is reported to the Chair of Governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and the Network Manager, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

Peer on Peer Sexual Abuse and Harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the 'Prevent' programme. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with 'Prevent' procedures.

Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Special Educational Needs Policy.

Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes
- Careful to avoid needlessly scaring or distressing pupils
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils
- Proportional to the actual or perceived risk
- Helpful to the pupils who are, or are perceived to be, at risk
- Appropriate for the relevant pupils' age and developmental stag
- Supportive
- In line with the Safeguarding and Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

Online Safety Training for Staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Behaviour Policy and the Safeguarding and Child Protection Policy.

Online Safety and the Curriculum

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

- PSHE
- RSHE
- Citizenship
- ICT / 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
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The DSL is 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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work

together to ensure the curriculum is tailored so these pupils 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL 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 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are 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 ensures 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 Safeguarding and Child Protection 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 Safeguarding and Child Protection Policy.

Use of Technology in the Classroom

The Harvey Grammar School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

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 always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

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.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Behaviour Policy.

Staff will use all smart technology and personal technology in line with the school's Behaviour Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils at times may use the internet in an inappropriate way.
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 will not be permitted to use smart devices or any other personal technology whilst in the classroom unless given permission to do so by the teacher.

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 discipline those involved in line with the school's Behavioural Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

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 4C's (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.

Educating Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

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
- 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 is raised in the following ways:

- Parents' Evenings
- Parents' Forums
- Twilight Training Sessions
- Termly Newsletters
- Online Resources

Filtering and Monitoring Online Activity

The Governing Body ensures the school's ICT network has appropriate filters and monitoring systems in place.

The Governing Body ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher and Network Manager undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are 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.

Requests regarding making changes to the filtering system are directed to the Headteacher. Prior to making any changes to the filtering system, the Network Manager and the DSL conduct a risk assessment. Any changes made to the system is recorded by the Network Manager. Reports of inappropriate websites or materials are made to the Network Manager immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and the Network Manager, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Staff Disciplinary Policy.

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

Network Security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the Network Manager. Firewalls are switched on at all times. The Network Manager reviews the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the Network Manager.

All members of staff have their own unique usernames and private passwords to access the school's systems.

Pupils are provided with their own unique username and private passwords.

Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. The school employs additional authentication software through Microsoft to reinforce password security.

Users inform the Network Manager if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher is informed and decides the necessary action to take.

Users are required to lock access to devices and systems when they are not in use.

Emails

Access to and the use of emails is managed in line with the Data Protection Policy.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to the Network Manager. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails are managed in line with the Data Protection Policy.

Social Media and Networking

Expectations

The expectations regarding safe and responsible use of social media and networking applies to all members of The Harvey Grammar School community.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of The Harvey Grammar School community are expected to engage in social media and networking in a positive, safe and responsible manner.

All members of The Harvey Grammar School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control pupil and staff access to social media whilst using school provided devices and systems on site.

Inappropriate or excessive use of social media and networking during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of The Harvey Grammar School community on social media, should be reported to the DSL and will be managed in accordance with our Safeguarding and Child Protection, Managing Allegations Against Staff, Anti-Bullying and Behaviour Policies.

Staff Personal Use of Social Media

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

Safe and professional behaviour will be outlined for all members of staff (including volunteers).

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites.

Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school

Members of staff are encouraged not to identify themselves as employees of The Harvey Grammar School on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL and/or the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with Pupils and Parents/Carers

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL and/or the Headteacher.

If ongoing contact with pupils is required once they have left the school, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.

Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL and/or the Headteacher.

Any communication from pupils and parents received on personal social media accounts will be reported to the DSL and/or The Headteacher.

Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies, including Anti-Bullying, Behaviour and Safeguarding and Child Protection. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

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

Official Use of Social Media

The Harvey Grammar School runs a limited number of social media accounts for example the HGS Sport Twitter account.

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

The official use of social media as a communication tool has been formally risk assessed and approved by the DSL and/or the Network Manager. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

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

Staff use setting provided email addresses to register for and manage any official social media channels.

Official social media sites are suitably protected and, where possible, run and linked to our website.

Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data Protection, Safeguarding and Child Protection.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Written parental consent will be obtained, as required.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving pupils will be moderated

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff Expectations

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

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

- always be professional and aware they are an ambassador for the school
- disclose their official role and position but make it clear that they do not necessarily speak on behalf of the school
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared
- always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws
- ensure that they have appropriate consent before sharing images on the official social media channel
- not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so
- not engage with any direct or private messaging with current pupils, parents/carers
- inform the DSL and /or Network Manager of any concerns, such as criticism, inappropriate content or contact from pupils

The School Website

The Headteacher is responsible for the overall content of the school website – he will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website.

Use of Devices

The Harvey Grammar School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-Bullying, Behaviour and Safeguarding and Child Protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

All members of The Harvey Grammar School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

All members of The Harvey Grammar School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

The sending of abusive or inappropriate messages or 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 Behaviour Policy and Staff disciplinary policy.

All members of The Harvey Grammar School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour, Safeguarding and Child Protection Policies.

Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Data Protection Policy, Safeguarding and Child Protection Policy and Managing Allegations Against Staff Policy.

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, unless permission has been given by the Headteacher, such as in emergency circumstances
- Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations

Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents/carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL.

Staff will not use personal devices:

- to take photos or videos of pupils unless permission has been given by the Headteacher, and will only use work-provided equipment for this purpose
- directly with pupils and will only use work-provided equipment during lessons/educational activities

If a member of staff breaches our policy, action will be taken in line with our Staff Disciplinary Policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

The Harvey Grammar School expects pupils' personal devices and mobile phones to be kept in a secure place and kept out of sight during lessons.

Mobile phones or personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a pupil breaches the policy, sanctions and interventions will be applied in relation to Appendix E 'Mobile Phone Procedures' of the Behaviour Policy.

Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our Behaviour Policy, Safeguarding and Child Protection Policy and Anti-Bullying Policy or could contain youth produced sexual imagery (sexting). The following would apply:

- Searches of mobile phone or personal devices will only be carried out in accordance with our Behaviour Policy and Safeguarding and Child Protection Policy
- Pupil's mobile phones or devices may be searched by a member of the Leadership Team, with the consent of the pupil or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our Behaviour Policy and Safeguarding and Child Protection Policy
- Mobile phones and devices that have been confiscated will be released to parents/carers
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our Anti-Bullying, Behaviour and Safeguarding and Child Protection Policies.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL.

Officially Provided Mobile Phones and Devices

Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/carers is required. In addition, occasionally school provided mobile phones/devices will be issued to staff where appropriate.

School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

School mobile phones and devices will always be used in accordance with the relevant policies.

Remote Learning

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites
- Direct parents to useful resources to help them keep their children safe online

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Monitoring and Review

The school recognises that the online world is constantly changing; therefore, the DSL, the Network Manager and the Headteacher conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The Governing Body, Headteacher and DSL review this policy in full according to the agreed schedule and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community