Success For All

Holly Lodge High School

College of Science

Online Safety Policy 2024-2025

Date Adopted:	April 2024
To be Reviewed:	April 2025
Signed by Governors	
Signed by Headteacher:	

Ambition | Opportunity | Community

On line Safety Policy

1. Policy Aims

The purpose of this online safety policy is to:

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

We identify that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2. Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- We believe that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as students, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school but is linked to member of the school.
- In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school.

2.1 Links with other policies and practices

This policy links with several other policies (but not limited to):

- Anti-bullying policy
- Acceptable Use Agreements (AUA) and the Code of Conduct/Staff behaviour policy
- Behaviour for Learning policy
- Safeguarding and Child protection policy
- Curriculum policies, such as: (PSHE), Citizenship and Relationships and Sex Education (RSE)
- GDPR
- Remote Learning Policy

This policy should also be read in conjunction with the school Vision Statement and Ethos of the School.

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; We will review this policy at least annually
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The DSL will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Debbie Southall, Deputy Headteacher has lead responsibility for online safety.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.
- Agilysis also has a lead role in ensuring the online safety of the school community.

4.1 The leadership and management team and governors will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running interrelated theme whilst devising appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that they are doing all that they reasonably can to limit children's exposures to risks from the school's IT system and therefore have suitable and appropriate filtering and monitoring systems are in place. They will have an awareness and understanding of the provisions in place and will work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that they regularly review the effectiveness of filters and monitoring systems; as schools increasingly work online, it is essential that children are safeguarded from

potentially harmful and inappropriate online material (including when they are online at home).

- Ensure that online safety is embedded within a progressive Personal Development curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- Recognise that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice, ideally annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.
- Communicate with parents regarding the importance of children being safe online, the systems being used in school and information regarding what their children are being asked to do online by the school.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools safeguarding responsibilities and that a coordinated approach is implemented.
- Liaise with staff (especially pastoral support staff, school nurses, IT technicians, mental health lead and SENCO) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique
- risks associated with online safety and have the relevant knowledge and up to date
- required to keep students safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms (My Concern).
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns to the SLT.

- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (termly) with the governor with a lead responsibility for safeguarding and online safety.

4.3 It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the schools safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that students are 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.
- Reinforce the school’s online safety messages when teaching lessons online

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the schools IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised. This includes using 2 factor authentication where available, unique passwords, not allowing users to re-use passwords and changing passwords frequently. Our additional security measures include; web filtering, spam filtering, network firewall, anti-virus, end point encryption and ransomware protection and online back ups.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

4.5 It is the responsibility of students to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to Acceptable Use Agreements.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

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

5. Education and Engagement Approaches

5.1 Education and engagement with students

- We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst students by:
- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in our Personal Development Curriculum.
- Online safety is also to be covered in each year of the IT/ Computing curriculum.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

We will support students to read and understand the acceptable use agreements in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms.
- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Providing Regular and up to date online safety education and training
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Students

- The school recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to students (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by Providing information and guidance on online safety in a variety of formats.
- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition and other school events.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use agreement and discuss the implications with their children.

6. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content.

- All members of the community will be directed to the DSL or headteacher in such circumstances.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- We require staff, parents, carers and students to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Sandwell Childrens Safeguarding Partnership.
- Where there is suspicion that illegal activity has occurred contact the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL or headteacher will contact the Police first to ensure that potential investigations are not compromised.

6.1 Concerns about Students' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns using the schools My Concern and other systems as outlined in the Child Protection and Safeguarding policy.
- The DSL (or deputies) will record these issues in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the SCSP thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

6.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the allegations policy.
- For any allegations regarding a member of staff's online conduct a consultation will be sort with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff code of conduct.

7. Safer Use of Technology

7.1 Classroom Use

Holly Lodge High 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, Email, Digital cameras, web cams and video cameras

- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and students complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their ability and understanding.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, students and visitors will read and sign an acceptable use agreement before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Holly Lodge High School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit student's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- We use Securus which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- We work with Agilysis and Securus to ensure that our filtering policy is continually reviewed.
- If students discover unsuitable sites, they will be required to:
- **Turn off monitor/screen and report the concern immediate to a member of staff.**
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies.

7.3.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
- Use of our monitoring systems such as Securus and staff monitoring. Reports are sent to the Safeguarding and DOSP team to investigate
- If a concern is identified via monitoring approaches we will will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

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

7.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.

- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

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

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or student's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of our school community.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices and processes, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.
- We will ensure that all students and staff included in images have given permission.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform members of the Safeguarding team if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents.

7.8.2 Student email

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

7.9 Management of Applications (apps) used to Record Children's Progress

We use SIMS and Classcharts to track students progress and share appropriate information with parents and carers.

- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard student's data:
- Only school issued devices will be used for apps that record and store students' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store students' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Holly Lodge High School.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the school are expected to engage in social media in a positive, safe and responsible manner.
- All members of Holly Lodge High School 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 student and staff access to social media whilst using setting provided devices and systems on site.
- The use of social media during setting hours for personal use is not permitted.
- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of the school community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct/ Staff behaviour policy as part of Acceptable Use Policy.

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 setting.
- Civil, legal or disciplinary action may be taken if staff are found to bring the profession or school community 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 setting.
- Members of staff are encouraged not to identify themselves as employees of our setting on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, 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 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 students and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with students and parents and carers

- Communication with children both in the ‘real’ world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children.

They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

- Any pre-existing relationships or exceptions that may compromise this, will be discussed with the headteacher (see *Staff Code of Conduct for further information*)
- If ongoing contact with students is required once they have left the setting, 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 students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the headteacher.
- Any communication from students and parents received on personal social media accounts will be reported to the Headteacher/DSL (or deputies).

8.3 Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded Personal Development Curriculum, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for students under this age.
- Any concerns regarding students use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.
- Students will be advised:
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- 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.
- To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

8.4 Official Use of Social Media

Holly Lodge High School official social media channels are a X 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 Headteacher.
- 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 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: antibullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- 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 students will be moderated if possible.
- Parents and carers will be informed of any official social media use with students; written parental consent will be obtained, as required.
- 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 professionals 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 setting, they will:
- Sign our acceptable use policy.
- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role but make it clear that they do not necessarily speak on behalf of the setting.
- 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 school, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, students, parents and carers.
- Inform the DSL (or deputies) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from students.

9. Use of Personal Devices and Mobile Phones

- We 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 setting.

9.1 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 child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.

- All members of Holly Lodge High 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 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.
- Mobile phones and personal devices are not permitted to be used on the school.
- 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.
- All members of Holly Lodge High School 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 or child protection policies.

9.2 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: confidentiality, child protection, data security and acceptable use.
- 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 and meeting times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Ensure that any content bought 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 and carers. Unless permission is sought with exceptional circumstances and the staff number hidden.
- Any pre-existing relationships, which could undermine this, will be discussed with the headteacher.
- Staff will not use personal devices:
- To take photos or videos of students and will only use work-provided equipment for this purpose.
- Directly with students and will only use work-provided equipment during lessons or educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations 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.

9.3 Students' Use of Personal Devices and Mobile Phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Holly Lodge High School expects students' personal devices and mobile phones to be switched off and out of sight during the school day.
- If a student needs to contact his/her parents or carers they will be allowed to use a school phone or use their own mobile during break and lunch only.
- Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

- Mobile phones or personal devices will not be used by students 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.
- If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Senior Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
- Students 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 student breaches the policy, the phone or device will be confiscated and will be held in a secure place for a parent to collect.
- Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with our policy.
- Students` mobile phones or devices may be searched by a member of the leadership team, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers.
- If there is suspicion that material on a student'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.