## Holme Grange School

## Whole School Policy Including EYFS

# E-Safety Policy

| Date: | Amendment: | Reviewed by: | Authorised by: |
|---|---|---|---|
| **September 2023** | **Next review due** | | |
| **August 2022** | **Reviewed** | **JCo** | **SMT Sept 22. Gov review pending** |
| **September 2021** | **Reviewed** | **JCo** | **SMT – 02.11.21 and passed to Governors** |
| **October 2020** | **Reviewed** | **JCo** | **SMT – 10.11.20** |
| **September 2019** | **Created** | **JCO** | **SMT – 11/02/2020** |

## Contents

## Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers the Headteacher 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. This is pertinent to incidents of cyber-bullying, or other e-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-Safety behaviour that take place out of school.

Holme Grange School adopts a zero-tolerance approach to any cyber bullying issues. All staff will challenge any abusive behaviours between pupils that comes to their notice. Staff will report any issues of this nature to the DSL immediately. Please read the Safeguarding and Child Protection policy for further details regarding dealing with child-on child abuse.

*UK Safer Internet Centre: appropriate filtering and monitoring*. Guidance on e-security is available from the National Education Network (NEN).

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

### Governors**:**

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The Governors will receive information about e-Safety incidents. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of this Governor will include:

- regular meetings with the designated safeguarding lead
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meetings

## Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day-to-day responsibility for e-Safety will be delegated to the Designated Safeguard Lead (DSL). The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Headteacher / Senior Leaders are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.

The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the DSL.

## The Designated Safeguarding Lead:

- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority - Berkshire West Safeguarding Children Partnership
- liaises with school technical staff
- receives reports of e-Safety incidents from the Head who makes a log of incidents to inform future e-Safety developments.
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team
- is trained in e-Safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:
    1. sharing of personal data
    2. access to illegal / inappropriate materials
    3. inappropriate online contact with adults / strangers
    4. potential or actual incidents of grooming
    5. cyber-bullying

## I.T. Manager / Technical staff:

The IT support team is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-Safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader; DSL for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

## Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the Staff Code of Conduct & Acceptable Use (Staff)
- they report any suspected misuse or problem to the Headteacher/Senior
- Leadership team; DSL for investigation/action/sanction
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-Safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Students / pupils

- are responsible for using the school digital technology systems in accordance with the Student Code for Acceptable Use which is in the school planners and distributed annually. All students in Prep School and Eaton Grange agree to the policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand behaviour policies and rules regarding the use of technology. They should also know and understand policies on bullying and how this relates to their online activities.
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

## Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-Safety campaigns/literature, this includes membership to the online safety platform: www.nationalonlinesafety.com

Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online student records
- mobile phones: these are not allowed to be used in the school playground area or in the EYFS area.

## Community Users

Community Users cannot access school systems. They will be given access to guest WIFI if needed.

## Policy Statements

## Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-Safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build resilience.

E-Safety is a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned e-Safety curriculum is provided as part of ICT/ computing/SMSC/PSHE (RSHE is covered within our PSHE programme) and other lessons and should be regularly revisited

Key e-Safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

Students are taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Students are educated to understand the Code for Acceptable Use (Pupils) and encouraged to adopt safe and responsible use both within and outside school

Staff are expected to act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is planned; it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and the School adopts filtering and content management to systematically support this process.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

## Education – parents/carers

Many parents and carers have only a limited understanding of e-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Policy documents
- Letters, newsletters, website,
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day, Parents' Conferences and talks
- Reference to the relevant web sites/publications, for example: www.swgfl.org.uk

www.saferinternet.org.uk
http://www.childnet.com/parents-and-carers
www.thinkuknow.co.uk
https://www.gov.uk/government/publications/education-for-a-connected-world
www.commonsensemedia.org

- Membership of National Online Safety https://nationalonlinesafety.com/enrol/holme-grange-school a platform which allows parents, teachers, and pupils to have access to a comprehensive suite of training programmes
- advice for parents and carers on cyberbullying

## Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's e-Safety knowledge and experience. This may be offered through e-Safety presentations which invite other schools or professionals, for example the biennial Parent Conference or collaboration with partner schools.

## Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

E-safety training is regularly made available to staff through EduCare.

An audit of the e- safety training needs of all staff is carried out periodically and it is expected that some staff will identify e-safety as a training need within their appraisal process.

All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the School e-Safety Policy and Acceptable Use Policy. The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

This e-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

The DSL will provide advice/guidance/training to individuals as required.

## Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-Safety/health and safety/child protection. This may be offered in a number of ways:

Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.

Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Use of the Educare and National Online Safety training platforms

## Technical – infrastructure/equipment, filtering and monitoring

The School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

School technical systems will be managed in ways that ensure that the School meets recommended technical requirements

There will be regular reviews and audits of the safety and security of school technical systems

Servers, wireless systems and cabling must be securely located and physical access restricted

All users will have clearly defined access rights to school technical systems and devices.

All users will be provided with a username and secure password by the IT support team who will keep an up to date record of users and their usernames. In accordance with Codes for Acceptable Use, users are responsible for the security of their username and password and will be required to change their password regularly.

The administrator passwords for the school ICT system, used by the IT support team must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

The IT support Team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

Internet access is filtered for all users. Illegal content (for example, child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and

internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

Impero protection. This monitors in real time the children's use of IT equipment looking for trends, activity and triggers which could indicate threat to life, or attempts to bypass security or protection systems.

The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc.)

School technical staff regularly monitor the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.

An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School systems. They will be given a login which does not allow any access to the school server. Holme Grange has a "guest" WIFI for such occasions.

An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.

An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on School devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (please refer to the School Privacy Notices)

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and

existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

No mobile phones are allowed to be visible or used in the Early Years areas. Please see the Staff Acceptable Use Policy. There is signage to remind visitors, parents and staff.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Where possible, images should be taken using School equipment. Where this is not practicable, use of personal devices must align with guidance as set out in the Code for Acceptable Use (Staff).

Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Students' full names will not be used anywhere on a website, twitter or Facebook, particularly in association with photographs.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and is fully GDPR compliant

## The school / school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Privacy Notice Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

## Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Transfer data using encryption and secure password protected devices.

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice.

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff

and students should use the school email service to communicate with others for School related matters/activity.

Users must immediately report, to the nominated person – in accordance with the School policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff and students or parents/carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used for these communications.

Students should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Social Media

All Social Media falls under the responsibility of one central accountable individual, this will be the Headteacher or a single designated member of staff appointed by the Headteacher.

There should be no other social media interactions on a whole school basis.

Use of closed communication channels, such as WhatsApp, are not permitted for school purposes or with students.

Our school has a duty of care to provide a safe learning environment for students and staff. The school could be held responsible, indirectly for acts of our employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

- School staff should ensure that:
- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

## User Actions

Users **shall not** visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children from Sexual Offences 2012
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986, Prevent strategy, The Counter-Terrorism and Security Act 2015
- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / school
- Infringing copyright
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)

- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming
- Commerce File sharing
- Use of social media
- Use of messaging apps
- Hacking
- Personal Apps
- Weapons
- Abortions advocacy groups
- Dating
- Malware

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

### Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Safeguarding including Child Protection Policy

### Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow School policies. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

### In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process? This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same device for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the **url** of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedure
- Involvement by Local Authority
- Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the device in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained for evidence and reference purposes.

## School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

## Related documents

- Keeping Children Safe in Education 2021
- Safeguarding including Child Protection Policy
- Tackling Bullying Policy

- Guidance for safer working practice for those working with children and young people in education settings 2020
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Staff Code for Acceptable Use
- Staff Code of Conduct
- Pupil Code for Acceptable Use
- Remote Learning Policy
- https://360safe.org.uk/
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf
- Cyberbullying Advice for Headteachers and School Staff
-

## Availability

This policy is made available to parents staff and pupils via the website (Parents), Every and SharePoint (Staff). A request may be made for the policy at the school office.

## Monitoring & review, policy into practice

We will review this Policy at least once every two years as well as if incidents occur that suggest the need for review.

**Appendix 2**
**1:1 device Policy**

Holme Grange School recognises that as technology develops more pupils have access to Internet enabled devices. We believe that these should be seen as a resource and provide an opportunity to enhance learning.

**General Information**

Access to the Holme Grange School wireless network, whether with school-provided or personal devices, is restricted. Access from personal devices is limited to Internet use only. Pupils will not have access to any documents which reside on the school network from their personal devices.

Access to the Holme Grange School wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the network also allows ICT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request. Pupils will be asked to sign a code of conduct agreeing to the conditions of using their own devices.

**Access to the Network**

To obtain access to the network pupils will have to ask their Head of School.
The technicians will check the device for viruses.
The network access password will be changed every half term.
A register of all student devices with network access will be kept by the ICT department.

**Guidelines**

**It is the expectation that pupils will not be required to bring their own device into school, the schools IT resources being sufficient for all educational activity.**
**In the near future pupils in Eaton Grange will be able to bring in their own devices to work from. This policy will be adapted to reflect this.**
**If after consultation with ALC and SLT, an agreed provision to enable curriculum access requires a pupil to bring in their own device the following applies.**

- Pupils are only allowed to work on the device that they have registered with the ICT Department
- Use of personal devices during the school day is at the discretion of teachers and staff. Pupils must use devices as directed by their teacher.
- The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. contacting parents, should not be allowed.
- The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.
- The use of personal devices falls under Holme Grange School's Code of Conduct which all pupils have to sign before bringing any personal device to school.
- Pupils shall not use personal devices outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.
- Pupils shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security

- Pupils shall not distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).
- Any digital images of students and staff on a device are considered personal data and as such are covered by the Data Protection Act. These images cannot be used or shared without prior written consent from the school or from the parent/guardian of the student involved.
- Devices will be inspected for inappropriate content as well as viruses. To ensure nothing is bought into the school. This will be carried out on a random basis thereafter.
- A check will be made to make sure the device has appropriate virus protection and has the latest updates installed (as well as a check for viruses and malware.
- Pupils must not bring in devices which have their own internet connection (i.e. 3G / 4G /5G) – an example of this is iPad with sim cards fitted as this could mean the children could potentially access the internet without any filtering or threat to life monitoring.

**Consequences for Misuse/Disruption**
(one or more may apply):

· Access to the wireless network will be removed.
· Device taken away for the period.
· Device taken away and kept by SMT until parent picks it up.
· Student is not allowed to use personal devices at school.

Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour Policy and will be dealt with in accordance with this policy.

**School Liability Statement**

Pupils bring their devices to use at Holme Grange School at their own risk.

Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

The school will not provide any secure facilities for storage of personal devices. Pupils are responsible for looking after their own device.
When the BYOD policy comes in to practice, pupils will have access to a secure charging locker for their device.

Holme Grange School is in no way responsible for:

- Personal devices that are broken while at school or on the way to/from school
- Personal devices that are lost or stolen at school or on the way to/from school
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
- Any Health and Safety compliance of personal devices e.g. correct wiring, plug etc.

Parents will be asked to ensure that they have adequate insurance for any device that is brought into school and they will be asked to sign a disclaimer.