**1.0 Background**

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students / pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This E-Safety policy should help to ensure safe and appropriate use. Technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the internet.

• The sharing / distribution of personal images without an individual’s consent or knowledge

• Inappropriate communication / contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video / internet games

• An inability to evaluate the quality, accuracy and relevance of information on the internet

• Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies.)

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

**2.0 Scope of the Policy**

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 out of school, but is linked to membership of the school.

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

**3.0 Roles and Responsibilities**

3.1 Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

• regular meetings with the E-Safety Co-ordinator

• regular monitoring of e-safety incident logs

• regular monitoring of filtering / change control logs alongside DSL (Designated Safeguarding Lead)

3.2 Head Teacher and Senior Leaders

• The head teacher is responsible 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 E-Safety Co-ordinator.

• The head teacher / Senior Leaders are responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

• The head teacher / 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 monitoring reports from the E-Safety Co-ordinator.

• The head teacher and 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.

3.3 E-Safety Co-ordinator alongside Designated Safeguarding Leads (DSL)

• 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

• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

• meets with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting / Governors Committee

. takes lead responsibility for monitoring the filtering of the IT systems

3.4 GHS / Technical staff

Our school has a managed computing service provided by an outside contractor. It is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school’s technical staff, as suggested below. It is also important that the managed service provider is fully aware of the School Acceptable Usage Policy.

GHS are responsible for ensuring:

• that the school’s computing infrastructure is secure and is not open to misuse or malicious attack

• that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant DFE-Safety Policy and guidance

• that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularly changed

* EXA is informed of issues relating to the filtering.

• the school’s filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix “Filtering Policy”)

• 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 / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /head teacher/ Computing Co-ordinator for investigation

• that monitoring software / systems are implemented and updated as agreed in school policies

3.5 Teaching and Support Staff

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 school Staff Acceptable Use Policy (AUP)

• they report any suspected misuse or problem to the E-Safety Co-ordinator /head teacher / Computing Co-ordinator / Class teacher for investigation

• digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities

• pupils understand and follow the school e-safety and acceptable use policy

• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• they monitor computing activity in lessons, extra-curricular and extended school activities

• they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

• in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

. Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

(NB. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop)

3.6 Pupils

Pupils:

• are responsible for using the school computing systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.

• 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

• 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.

3.7 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of computing than their children. The school will therefore take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

• accessing the school website

**4.0 Policy Statements**

4.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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 their resilience.

E-Safety education will be provided in the following ways:

• A planned e-safety programme will be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of computing and new technologies in school and outside school

• Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

• Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of computing, the internet and mobile devices both within and outside school

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Staff should act as good role models in their use of computing, the internet and mobile devices

4.2 Education – Parents / Carers

Many parents and carers have 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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

\* Class Dojo messaging which is limited to parents and staff

• Letters, newsletters, website

• Parents evenings

4.3 Education & Training – Staff

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:

• A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

* The E-Safety Co-ordinator will receive regular updates through attendance at training sessions and by reviewing guidance.

• This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.

• The E-Safety co-ordinators will provide advice as required to individuals as required.

4.4 Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any committee involved in computing / e-safety / health and safety / child protection.

**5.0 Technical – infrastructure / equipment, filtering and monitoring**

(NB. while the school has a managed computing service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school.)

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. It will also ensure that the relevant people will be effective in carrying out their e-safety responsibilities.

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

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

• All users will have clearly defined access rights to school computing systems.

* The “master / administrator” passwords for the school computing system are only to be known by GHS, ensuring that more than one user has sole administrator access.

• The school maintains and supports the managed filtering service provided by EXA

• In the event of GHS (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the head teacher (or other nominated senior leader).

• Any filtering issues should be reported immediately to E-safety lead/ DSL who will contact GHS/ EXA support.

• Requests from staff for sites to be removed from the filtered list will be considered by the head teacher/ GHS and E-safety Officer. If the request is agreed, this action will be recorded.

• GHS and the Designated safeguarding leads regularly monitor and record the activity of users on the school computing 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 e-safety incident to the E-Safety Co-ordinator.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

• An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices without permission from the head teacher, Senior Leaders or the E Safety Co-ordinator.

• The school infrastructure and individual workstations are protected by up to date virus software.

• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**6.0 Curriculum**

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of computing across the curriculum.

• in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

* It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that GHS 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 and sanctioned by the head teacher.

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

**7.0 Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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 pupils 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.

• Staff 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. Staff should not take videos/ photos on personal devices such as mobile phones etc.

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

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

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

• Pupils’ full names will not be used anywhere on a website, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or class dojo.

**8.0 Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• Kept no longer than is necessary

• Processed in accordance with the data subject’s rights

• Secure

• Only transferred to others with adequate protection.

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.

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

•. Staff should use only the school email service or class dojo to communicate with others including parents.

• Users need to be aware that email communications and class dojo will be monitored

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

• Any digital communication between staff and pupils or parents / carers (email, dojo) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

• Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

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

School Pro limited act as our data protection and GDPR professional advisors and we defer to them if issues arise and for guidance.

**9.0 Unsuitable / inappropriate activities**

Some internet activity e.g. accessing child abuse images, distributing racist material or Cyber-bullying is illegal and is obviously banned from school and all other computing systems and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those 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 certain internet usage as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| **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** |  |  |  |  | MCj04347130000[1] |
| **promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation** |  |  |  |  | MCj04347130000[1] |
| **adult material that potentially breaches the Obscene Publications Act in the UK** |  |  |  |  | MCj04347130000[1] |
| **criminally racist material in UK** |  |  |  |  | MCj04347130000[1] |
| **pornography** |  |  |  | MCj04347130000[1] |  |
| **promotion of any kind of discrimination** |  |  |  | MCj04347130000[1] |  |
| **promotion of racial or religious hatred**  |  |  |  | MCj04347130000[1] |  |
| **threatening behaviour, including promotion of physical violence or mental harm**  |  |  |  | MCj04347130000[1] |  |
| **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** |  |  |  | MCj04347130000[1] |  |
| **Using school systems to run a private business** |  |  |  | MCj04347130000[1] |  |
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by EXA and / or the school** |  |  |  | MCj04347130000[1] |  |
| **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions** |  |  |  | MCj04347130000[1] |  |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** |  |  |  | MCj04347130000[1] |  |
| **Creating or propagating computer viruses or other harmful files** |  |  |  | MCj04347130000[1] |  |
| **Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet** |  |  |  | MCj04347130000[1] |  |
| **On-line gaming (educational)** |  |  |  | MCj04347130000[1] |  |
| **On-line gaming (non-educational)** |  |  |  | MCj04347130000[1] |  |
| **On-line gambling** |  |  |  | MCj04347130000[1] |  |
| **On-line shopping / commerce** |  |  |  | MCj04347130000[1] |  |
| **File sharing** |  |  |  | MCj04347130000[1] |  |
| **Use of social networking sites** |  |  |  | MCj04347130000[1] |  |

**9.1 Responding to incidents of misuse**

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

If any apparent or actual misuse appears to involve illegal activity ie.

• child sexual abuse images

• adult material which potentially breaches the Obscene Publications Act

• criminally racist material

• other criminal conduct, activity or materials

Then the relevant authorities will be contacted.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is 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.

**10.0 Review of this Policy**

This policy will be reviewed by the SIC every 3 years or earlier if required.

**Date ratified by Governors: (Due to go to Governors on 3.10.23)**

**Review Date: October 2026**