Gartree High School
E-safety & ICT acceptable use Policy

- Introduction and Purpose
- Scope of Policy
- Our School's Technology Systems and Infrastructure
- Expectations on the use of the school's technologies
- Standards and Inspection
- Working in partnership with Parents and Carers
- Reporting Abuse
- Education and Training
- Appendices of the E-safety Policy
    - Appendix A: Acceptable Use Policy Agreement Staff
    - Appendix B: Acceptable Use Policy Agreement Student

Introduction and Purpose

Gartree High School recognizes the critical role digital technologies play in all our lives and their growing importance in the lives of children and young people including their contribution to education and learning. This policy balances our desire to ensure that our young people become confident, competent and safe users of technology with the need to protect the school's systems and network. It shapes how we to ensure the school's online procedures keep children and young people safe, and how we to teach everyone about online safety, in and outside of school. It provides staff and volunteers with the overarching principles that guide our approach to online safety and ensures that, as an organisation, we operate in line with our values and within the law in terms of how we use technology.

Gartree High School places a high priority on ensuring children and young people never experience abuse of any kind. In our connected world this means ensuring that children and young people understand how to behave safely, understand what to do and what not to do to keep themselves safe, and understand the need to show respect to others, and finally understand what to do if they are threatened. We include cyber security in our approach to E-safety and set very high standards for both pupils and staff so that we minimise the threats of unauthorised access to people's devices, many of which contain cameras, the threats of theft or damage and so we prevent unauthorised access to the organisational and personal data we store in the school or online or that children and young people store on their devices. The school was fortunate to have suffered from a serious cyber security incident that impacted every system we use but did not affect the school's ability to function, the security of its data, or its reputation. Our good fortune was a combination of the backup policies and practices in place at the time, the magnificent efforts of the staff and the Leicestershire police, and the timing of the incident at the start of a holiday. That lucky combination enabled us to recover with minimal disruption but with some cost and the lessons learned from the incident contribute to the desire of both the school leadership team and the governing body to ensure that we do everything we can to avoid future incidents. We do this partly by ensuring everyone is practicing good E-safety and is aware of cyber risks and that we are adequately prepared in the event of a cyber incident. Schools face specific risks and have clear responsibilities for the use of ICT systems and data security. This policy is informed by the need to be compliant with the General Data Protection Regulations (GDPR) and the pupil safeguarding duties defined in Keeping children safe in education (DfE, 2022).

In some circumstances we will assist some pupils with technology devices and access to ensure an equitable learning experience for all pupils and we may provide additional help to parents and carers. We do this because we recognize the critical role technology plays in our society and the need to ensure equitable access to opportunities for learning.

This policy will need to be updated on a regular basis. The cyber security threats facing schools continue to grow and emerging evidence of the harm that social media can have on young people may inform changes. Currently there is an increasing role in education for Artificial Intelligence and Machine Learning in providing personalized automated guidance and feedback and we will continue to seek to ensure that all our pupils are fully equipped and able to gain the benefits of these new applications of technologies, while understanding and being informed about potential biases, dangers and risks.

Where appropriate we will also engage carers and parents to ensure they are fully informed about opportunities and able to use technologies, including the systems we provide. We will also share information so carers and parents understand some of the risks that exist and so that they can play a full active and informed role in safeguarding children and promoting E-safety.

The nominated senior person for the implementation of the School's E-Safety policy is Edward Wilson, the Designated Senior Lead for Child Protection.

Scope of Policy

This policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers and any community members or visitors

This policy should be read alongside our policies and procedures for safeguarding and child protection and our welfare procedures for responding to concerns about a child or young person's wellbeing, as well as our procedures for dealing with allegations of abuse made against a child or young person and for managing allegations against staff and volunteers. It aligns with our anti-bullying policy and the procedures for photography and image sharing.

Gartree High School will ensure that the following E-Safety elements are in place:

- clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person and an auditable reporting procedure for cases of abuse and misuse.
- support and training for all staff and volunteers on dealing with all forms of online abuse, including online bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- providing supervision, support and training for staff and volunteers about online safety and best practices for E-Safety and cyber security
- regular reviews and updating of the security of our information systems
- procedures that ensure that user names, logins, email accounts and passwords are used as effectively and safely as possible
- storing data which contains personal information about the adults and children who are involved in our organisation as securely as possible and only sharing this as appropriate
- gaining written permission before using images of children, young people and families and only using these images for the purpose for which consent has been given
- examining and risk assessing any social media platforms and new technologies before they are used within the school
- deploying specific systems to monitor and enforce E-Safety and cyber security policies and procedures so we can audit and inspect their consistent use (for example email quarantine and end user device protection)
- testing systems and our network, including penetration testing and attack simulations
- defining specific agreements for acceptable use for all staff and pupils
- restricting the use of devices that pupils bring to school (our 'no phones' policy)
- adequate supervision of pupils when using the internet and technologies at school;

- education that is aimed at ensuring pupils understand the principles of technology and the internet so they can safely use technologies

Expectations on the use of the school's technologies

Gartree High School uses a range of systems and technologies in a controlled and managed environment. We also use service providers to ensure the systems and technologies are reliable, safe and secure and to enforce our policies. All users of our systems, network and devices should understand that everything is monitored and controlled. We set and enforce policies to monitor what people are doing and to restrict use and ensure any user who is using our systems and network are doing so appropriately.

Gartree High School will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that sees the welfare of the child as paramount. To this end, we expect any organisation using the school's technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and report any concerns.

Gartree High School expects all staff and pupils and any other users of it's technologies to use these technologies responsibly. Users shall not browse, make, post, comment, link, download, upload, share or pass on material, that contains or relates to:

- indecent images of children;
- the promotion of any kind of discrimination or hatred such as that in respect of race, nationality or ethnicity, religion or belief, disability, sex including misogyny, gender reassignment

The school monitors the use of its technology and may need to report users to the police or make a referral to the Anti-terrorism PREVENT programme. The school may need to share personal information to ensure, for example, that a person at risk of radicalisation is given appropriate support.

We expect pupils to respect and comply with age restrictions that service providers put in place and not to seek to circumnavigate them or help others to do so, and we expect parents and carers to help ensure compliance with this.

The School recognises that in certain planned curricular activities, access to sites that would otherwise be deemed inappropriate may be appropriate and beneficial for an educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and supported by senior leaders, so that the action can be justified if challenged.

<u>In addition, users may not:</u>

- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes and passwords;
- use the schools for running a private business or intentionally interfere with the normal operation of the schools' systems or wifi network with a sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of

small files or any activity that causes network congestion) that substantially hinders others
- use the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment) or continuing to use an item of networking software or hardware after the school has requested that use cease because it is causing disruption to the correct functioning of the system;

Users must

Follow cyber security best practices, educating themselves about risks and protecting the school's systems and networks. In the same way that users must not assist others with unauthorised access to school facilities and premises, users must not assist others to access and use the school's technology services or network and must take reasonable steps to avoid the introduction of viruses or unauthorised and malicious access.

Users must ensure that they protect their data and their work by using the recommended storage and backup facilities. Users must not waste staff effort or network resources, including time spent managing end user devices or systems by:

- corrupting or destroying their own or other users' data;
- violating the privacy of other users;
- disrupting the work of other users

The school operates a no mobile phone policy for students. Staff and other users should only use mobile or independently connected devices in ways that are fully compliant with this policy.

Reporting Abuse

There may be occasions when either a pupil or an adult within the school receives an potentially dangerous or abusive email or accidentally accesses a website that contains abusive material or a virus or malicious code. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident immediately and seek help.

The School also recognises that there will be occasions where pupils will be the victims of inappropriate behavior that could lead to possible or actual significant harm, in such circumstances the school's safeguarding procedures should be followed.

Cyberbullying – Cyberbullying is the use of technology, internet and/or social media apps to cause repetitive and intentional harm to another. As a school we will not tolerate this and educate all of our students of this through PSHE lessons and the Tutorial programme. Any incidents will be dealt with in accordance with our Bullying policy (please see this for more information). For the avoidance of doubt the cyberbullying policy is in force for all pupils 24 hours a day 7 days a week throughout the whole year including weekends and holidays.

If inappropriate material is accessed, users are required to immediately report this. Young people must report it immediately to the first available member of staff. Adults must immediately report it to their line manager. The timing of any report will be considered and can be taken into account when considering an appropriate response.

Education and Training

Gartree High School recognises the need for all our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely. To this end, Gartree High School will:

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.

- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.

- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

- Teach cyber security skills and seek to ensure pupils, staff and parents are safe in the use of the school's systems and that they can transfer this learning to their wider lives.

Monitoring, audit and sanctions

Gartree High School is continuously monitoring its systems and networks and will run regular exercises to check that this policy and the required procedures are working well in order to ensure that users follow best practices and are working effectively and safely and that the risks to pupils staff and the school are minimised. Gartree High School will audit the use of its systems and the use of the Internet through its network and managed end user devices in order to ensure compliance with this policy.

We filter access to the internet so inappropriate sites are blocked and we can add sites to block as they are discovered or reported by staff or pupils. We use image technology to block offensive pictures before they are displayed. We stop any users who are seeking to circumnavigate these restrictions by using an anonymous proxy, by detecting and preventing their use. We actively monitor screens and pupil input including the detection of phrases which could constitute cyber-bullying and similar misdemeanours. Our cyber security technology for threat detection scans emails and uses keyword detection.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

Child / Young Person;

- The child/young person will be subject to the disciplinary process defined by the behaviour policy of the school, which could include the use of school systems, the internet and email being withdrawn;
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies

Adult (Staff and other adult users)

- The adult will be subject to the staff disciplinary process, if it is deemed he/she has breached the policy;
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies

Working in Partnership with Parents and Carers

Gartree High School is committed to working in partnership with parents and carers and understand the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere. Communication with school is vital for the partnership to be a success. We strongly encourage parents and carers to download the 'My Child at School' (MCAS) app as the school use this to safely provide invaluable information about attendance, homework and payments, as well as any behaviour and merit points. Teachers may also post relevant information within this app. The MCAS app alongside the school website and our social media channels are the main safe communication channels with parents and carers.

We at Gartree High School also appreciate that there may be some parents who are concerned about the use of technologies or who have specific requests and in such circumstances school staff will seek to engage parents and carers, explore concerns and suggest appropriate actions. The school seeks to ensure all pupils become organised self-starters and we encourage independent study and responsibility in our students. Parents and carers will not have full oversight of what their children are doing and this is intentional and by design. We except older students to have developed more of their self-management and independence and we do not seek to provide parents with what might be regarded as unnecessary surveillance capabilities through their use of the school's systems.

Appendices of the E-safety Policy

ICT Acceptable Use Policy Agreement - Staff

Introduction

New technologies have become integral to the lives of students in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement Staff

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications and that such use is not confidential.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, its learning etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of via EW, HMB, BR, SS or the network manager.
- I will not use a personal device to record images and I will not share images of others without their consent.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- I will only communicate with students online via the school systems. Any such communication will be professional in tone and manner. I will not use personnel e-mail or social networking to communicate with pupils
- I will only communicate with parents / carers using the school systems. Any such communication will be professional in tone and manner. I will not use personal e-mail or social networking to communicate with parents / carers
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that pupil details must not be sent via the external email system.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines

Signed		Date	

Acceptable Use Policy Agreement Pupils

I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.

I will not give out any personal information online, such as my name, phone number or address. I will not reveal my passwords to anyone. I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents or carers. If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to any member of staff.

I will not send anyone messages or material that could be considered threatening, bullying, offensive or illegal. I will not deliberately browse, download or upload material that could be considered offensive or illegal. If other pupils share such material with me then I will report it immediately to an appropriate adult. I understand that if friends share messages and pictures with me I should respect their privacy and

I understand that my internet use at Gartree High School will be monitored and logged and can be made available to staff. I understand that these rules are designed to keep me safe and that if I choose not to follow them, Gartree High School may contact my parents/carers and I may face sanctions including the loss of access to systems and devices.

Signed		Date	