Gatehouse School
E-Safety Policy

Policy Name	e-Safety Policy	**Last Review Date**	Spring 2023
Status	Mandatory	**Governors Review**	Spring 2023
		Next review	Spring 2024

Including the Code of Conduct for Pupils for Online Sessions on Remote Working Platforms

Appendix A: Acceptable IT Use - Staff Agreement
Appendix B: Remote Provision Protocol for Teaching Staff
Appendix C : Correct procedures for using Zoom for Teaching staff:

Introduction

Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, watches, computers, laptops and tablets – all of which form a part of children and young people's online world. The internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks.
E-safety forms a fundamental part of our safeguarding and child protection measures.

This policy will consider all current and relevant issues linked to e-safety, in a whole school context, linking with other relevant policies, such as the Safeguarding & Child Protection (including Prevent), Behaviour for Learning and Anti-Bullying policies.

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 the school are bound.

Through our e-safety policy, we ensure that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and

outside school. We also have a responsibility to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

The implementation of this policy will be monitored by the Headteacher, SLT and Safeguarding lead. The policy will be reviewed annually and updated according to newly published legislation.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Heateachers, to such an 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 outside of the school, but is linked to membership of the school.

There are increased 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 of incidents of inappropriate e-safety behaviour that take place out of school.

Online-abuse

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, watches, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).
It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be re-victimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline.
Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse

- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The link Governor for Safeguarding also acts as e-safety governor and will meet and work together with the Headteacher, DSL and Technology Services Provider representative to review all related policies, practices and procedures.

Designated Safeguarding Lead

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 and procedures
- Has training to demonstrate she understands the unique risks associated with on-line safety
- Can recognise the additional risks that learners with SEND face online.
- Ensures that all staff are provided with on-line safety training at induction and regular intervals
- 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 LADO
- Liaises with the ICT teacher
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, meets regularly with the Headteacher to discuss current issues, review incident logs and filtering/change control logs
- Reports regularly to the rest of the Leadership Team
- Meet and work together with the Headteacher, Governors and Technology Services Provider representative to review all related policies, practices and procedures.

Vizst Technology Services:

The IT Services provided by Vizst Technology are responsible in conjunction with the School's IT Technician 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 access the network and, where possible, devices through a properly enforced password protection policy, in which passwords are regularly changed
- That filtering and monitoring is applied and updated termly and that its implementation is not the sole responsibility of any single person
- That they provide filtering and monitoring reports and complete actions following concerns raised and carry out checks to the system
- That filtering and monitoring is applicable to devices used off site
- 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 monitoring software/systems are implementation and updated as agreed
- That they meet and work together with the Headteacher, DSL and Governors to review all related policies, practices and procedures.

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, procedures and practices
- They report any suspected misuse, concern or problem to the Headteacher or DSL for investigation
- All digital communications with pupils and parents should be on a professional level and only carried out using official school systems; all communication with pupils should be to their school email address
- E-safety issues are embedded in all aspects of the curriculum and other activities

Designated Person for Safeguarding

The Designated Person for Safeguarding should be trained in e-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Parents

Parents 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, the School website and information about national/local e-safety campaigns/literature. 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 images taken at school events

- Access to parents' sections of the website

Policy Statements

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

- A planned e-safety curriculum will be provided as part of the PSHE curriculum and is covered in further detail as part of every year group's Computing curriculum.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils will 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

Education - Parents

Many parents 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:

- Information evenings
- Letters, newsletters, website
- High profile events/campaigns eg. Safer Internet Days

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, as part of their training in Safeguarding. This will be regularly updated and reinforced.

- All new staff will receive e-safety training as part of their induction programme, linked to their Safeguarding training, 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.
- The DSL will provide advice/guidance/training to individuals as required.

Training - Governors

Governors should participate in e-safety awareness sessions, in school training sessions, eg. for staff or parents.

<u>Technical - infrastructure/equipment, filtering and monitoring</u>

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. The named responsible persons for filtering and monitoring are:
Gatehouse SLT Member- Fiona Tighe DSL
Gatehouse Governor- Joanna Scott

- Gatehouse technical systems will be managed in ways that ensure that the school meets all the recommended technical requirements, including filtering and monitoring, across all devices.
- There will be an annual review and audit of our safety and security of the schools technical systems. There will be a review of the system if new technology is installed, if a risk is identified or if there is a change in working practice.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Staff will not leave their computers or devices on when they are not in the room.
- 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 Vizst who will keep an up to date record of users and their usernames. Users are responsible for
- the security of their username and passwordThe “master/administrator” passwords for the school ICT system, used by Vizst must also be available to the Bursar
- Vizst 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. Filtering is not 100% effective and monitoring of use will include physical live viewing of systems, user log scrutiny and individual device monitoring.
- Illegal content (child sexual abuse images) is filtered by actively employing Sophos web filtering. Content lists are regularly updated and internet use is logged and regularly monitored by Vizst.
- Harmful and inappropriate content will be unblocked , without unreasonably impacting teaching and learning.

- There is a clear process in place to deal with requests for filtering changes- staff send an email to Vizst and a log is kept of requests. The DSL oversees the unblocking request log as part of the monitoring strategies.
- The school has provided enhanced/differentiated user-level filtering
- Vizst staff monitor and record usage of the school technical systems and users are made aware of this in the Acceptable Use Policy
- Users report any actual/potential technical incident/security breach to Vizst
- 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.
- The school infrastructure and individual workstations are protected by up to date virus software

Data Protection

Please see the Data Protection Policy

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 data may be recovered using the back-up system. Users should be aware that email communications are accessible by the Headteacher in connection with a concern or an investigation. Staff and pupils should therefore use only the school email service to communicate with others.
- Any digital communication between staff and pupils or staff and parents must be professional in tone and content. These communications may only be sent on official (monitored) school systems. Staff personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be taught about e-safety issues, such as risks attached to the sharing of personal details. They will 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.

Pupils will be taught:

- **How to evaluate what they see online**
- **How to recognise techniques used for persuasion**
- **Online behaviour**
- **How to identify online risks**

- **How and when to seek support**

<u>Potential Harms covered include:</u>

- **Age restrictions**
- **Content: How it can be used and shared**
- **Disinformation, misinformation and hoaxes**
- **Fake websites and scam emails**
- **Fraud (online)**
- **Password phishing**
- **Personal data**
- **Persuasive design which keeps 'users online for longer than they might have planned or desired'**
- **Privacy settings**
- **Targeting of online content**
- **Abuse (online)**
- **Challenges [to do something and post about it]**
- **Content which incites…hate, violence**
- **Fake profiles**
- **Grooming**
- **Live streaming**
- **Pornography**
- **Unsafe communication**
- **Impact on confidence (including body confidence)**
- **Impact on quality of life, physical and mental health and relationships**
- **Online vs. offline behaviours**
- **Reputational damage**
- **Suicide, self-harm and eating disorders**

When teaching about these safeguarding topics (and others), staff will be mindful that there may be a child or young person in the lesson who is or has been affected by these harms. During or after a lesson, a pupil may be prompted to disclose about something that may have happened online.

Staff will consult with the Safeguarding lead and Head of Pastoral Care when considering and planning any safeguarding related lessons or activities (including online) as they will be best placed to reflect and advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

Social Media - Protecting Professional Identity

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 and 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 pupils, parents 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

The school's use of social media for professional purposes will be checked regularly by the DSL to ensure compliance with the e-safety 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 policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible use 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 computer 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 computer 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 (web address) 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 procedures
    - Involvement by Local Authority or national/local organisation (as relevant)
    - Police involvement and/or action

- If the 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 Publication Act
    - Criminally racist material
    - Other criminal conduct, activity or materials
- Isolate the computer 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 Safeguarding purposes. The completed form should be retained by the group 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.

Incidents of misuse by pupils will be dealt with in accordance with the Behaviour Policy. If pupils deliberately access or try to access material that could be considered illegal, the matter will be referred to the Police. As a consequence, for serious misuse of the school's IT systems, access to the system may be restricted/withdrawn.

Incidents of misuse by staff will be dealt with in accordance with the Disciplinary Procedure. If staff deliberately access or try to access material that could be considered illegal, the matter will be referred to the Police.

Code of Conduct for Pupils for Online Sessions on Remote Working Platforms

This code of conduct outlines what we expect of pupils during online sessions.

Much of this echoes our expectations of pupils in lessons when in school and all of it is designed to help pupils gain the most benefit from online learning.

- I will only use google classroom and my school email for the purposes of online learning and will only browse, download, upload or forward material that is related to my learning and as directed by my teachers.
- I will not use my school email to create groups, initiate calls or initiate meetings and will end sessions when the teacher tells me to do so.
- I will check my google classroom regularly, with the help of my parent or carer, to keep track of online sessions and learning.

- During live online sessions my parent/carer will be in the vicinity, either in the room or a nearby room, with the door open.
- I understand that online sessions will be recorded but that the recordings will never be made public.
- I will not take photos of my screen or record online interactions in any way.
- I will make sure that my communication in the online learning environment is always supportive of my learning and the learning and wellbeing of others.
- When taking part in an online sessions I will make sure that
    - my environment is quiet and free from distractions
    - the background (and foreground) is appropriate (Be mindful of what is visible behind you/in front of you)
    - I am suitably dressed.
    - I remain attentive.
    - I communicate in a courteous way at all times to both teachers and fellow pupils. (Remember what we always say about social media, when you type something, 'it's always there and you can't take it back'. So be careful of what you say and write)

Parent's information about zoom 1-1 teacher meetings

- The teacher will host the 1-1 meetings with pupils via zoom.
- The parents or carers can access the appointment system through a link the teachers will send out to the child's email account. The teacher will then send through the meeting ID and password.
- The appointments are scheduled to last for 10 minutes.
- To make this system manageable please leave at least 2 hours between making the appointment and its scheduled time.

Appendix A:

Acceptable IT Use - Staff Agreement

Staff must be fully aware of their professional responsibilities when using information systems in regard to their work at the school. Staff should consult Gatehouse School's e-Safety Policy for further information and clarification.

Note: The term ‘information systems’ is used here to cover both hardware and software, and ‘the school’ to mean Gatehouse School.

- The information systems are the school’s property, and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role; this includes the use of internet access e.g. social media sites.

- I understand that the school’s information systems should not be used for private purposes, without specific permission from the Headteacher.

- I understand that the schools information systems provided to staff are for staff use only. Pupils are not to be allowed to them at any time.

- I understand that the school may monitor my information systems and internet use to ensure policy compliance.

- I will ensure that any personal data is kept secure and is used appropriately, whether in the school, taken off the school premises or accessed remotely.

- I will not use or set up any social network, Youtube or other online resources relating to activities at the school, unless I have the prior consent of the e-Safety Group.

- At no time will I bring into disrepute the name of the school on any social networks.

- I will not breach the **Social Media - Protecting Professional Identity** statement and content.

- I will respect copyright and intellectual property rights, and seek advice when unsure.

- I will report any incidents of concern regarding children’s safety to the Designated Safeguarding Lead.

- I will ensure that any electronic communications with pupils are compatible with my professional role. I will make no contact with pupils via social media sites, nor accept them as ‘friends’ on my own sites.

- I will promote e-Safety with students in my care, and will help them to develop a responsible attitude to system use and to the content they access or create.

- I will keep all data and information related to the school, students and colleagues confidential.

- I will return my computer and all associated equipment to Gatehouse School on the last day of my employment.

- I have read the school's Safeguarding and Child Protection Policy
- I have read KCSiE 2020 Part 1 and Annexe A

I have read, understood and agree with the Acceptable IT Use Policy.	
Full Name:	
Signed:	Date:

Appendix B: Remote Provision Protocol for Teaching Staff

Specific guidance related to remote provision and live sessions

The only forum on which live sessions should take place is on Zoom (see Appendix 1 Correct Procedures for using Zoom)

1. All live sessions must be recorded. This is for safeguarding reasons.
2. When admitting children into your zoom sessions do this individually from the waiting room so you are sure you recognise every child's contact details.
3. Do not have 1:1 conversations on video, except for scheduled 1:1 meetings.
   In live group sessions there must be at least 2 pupils present before they begin. A separate protocol is in place for those who normally work 1:1 with pupils (music teachers, SEN lessons etc)
4. To encourage normal working hours please do not post on any online provision after 18:00 or before 07:00am.
5. If a pupil contacts you via google classroom and a response is required then you should respond within 2 working days.
6. When recording or live streaming sessions, make sure the background is neutral and nothing personal or inappropriate can be seen or heard in the background:
   a. No pictures of children on walls etc
   b. Be mindful of what is visible behind you/in front of you
   c. Close all unnecessary programmes on your computer, particularly email, CPOMS.
   d. Do not have other people in the room when you are making a video or live streaming
7. Make sure that you are suitably attired.
8. When a zoom session is taking place, this must be hosted by the teacher.

Conduct the conversation/session following the same professional protocols as you would in a 'normal' lesson.

Do not use personal accounts.

Make sure that phone calls do not reveal personal phone numbers.

In everything we do, we adhere to the expectations as set out in the Staff Code of Conduct. Here are the main sections that are relevant to our distance provision protocols:

STAFF BEHAVIOUR POLICY / CODE OF CONDUCT

The aim of the Staff Behaviour and Code of Conduct policy is to provide clear guidance about behaviour and actions so as to not place pupils or staff at risk of harm or of allegation of harm to a pupil.

1. *All staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. They should adopt high standards of personal conduct in order to maintain the confidence and respect of their peers, pupils and the public in general. An individual's behaviour, including use of language, either in or out of the workplace, should not compromise her/his position within the work setting or bring the school into disrepute.*

2. *Communication with Pupils*
   Staff and volunteers must not give their personal details such as home/mobile phone number; home or email address to pupils unless the need to do so is agreed with senior management.

3. *Confidentiality*
   There are some circumstances in which a member of staff may be expected to share information about a pupil, for example when abuse is alleged or suspected. In such cases, individuals have a duty to pass information on without delay to those with designated pupil protection responsibilities.

4. *Personal Appearance*
   A person's dress and appearance are matters of personal choice and self-expression. However staff must ensure they are dressed decently, smartly, safely and appropriately for the tasks they undertake.

5. *Use of images of children*
   When using an image the following guidance must be followed: images must be securely stored and used only by those authorised to do so. Be clear about the purpose of the activity and about what will happen to the photographs or images when the lesson/activity is concluded, ensure that all images are available for scrutiny in order to screen for acceptability, be able to justify the images made, do not take, display or distribute images of pupils unless there is consent to do so.

6. *Social media*
   Staff must not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which could be considered inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

The whole document is part of the Child Protection, Safeguarding and Staff Code of Conduct, available on our website if you need to refer to it.

Appendix C

Correct procedures for using Zoom for Teaching staff:

- Log in to Zoom by clicking on 'sign in with Google' and using your school account, you should then be able to click on 'my account' in the top right corner, followed by 'settings' in the list to the left.
- The first two options are Host video and Participant video. Turn these OFF. This will mean that participants (including yourself) will be able to join the meeting, then turn on their camera when they are ready to.
- Audio Type can be left as it is to allow for different devices that children and staff may have to be using at this time.
- Join Before Host should be OFF.
- Both Use Personal Meeting ID settings should be OFF.
- Only Authenticated Users Can Join Meetings... should be ON.
- ALL AVAILABLE PASSWORD SETTINGS should be ON.
- Embed password in meeting link... should be OFF.
- Mute participants upon entry should be ON (for the same reasons as having video disabled when first joining meetings).
- ALL CHAT FUNCTIONS should be OFF.
- File Transfer should be OFF.
- Screen Sharing must be OFF.
- Disable desktop/screen share for users should be ON.
- All settings between this point and Waiting Room should be OFF.
- WAITING ROOM should be ON. (Another key feature, this means that when pupils join the meeting, you have to approve them before they appear. This is easy for us, as we just need to look for the gatehouse email address. DO NOT ALLOW ACCESS TO ANY OTHER EMAIL ADDRESS.When logged in to Zoom, go to settings as before, then click on the 'Recording' tab at the top of the page.
- Local recording should be on.

- Hosts can give participants the permission to record locally should be unchecked (off).
- Automatic recording should be on.
- Videos will be automatically saved to the device being used to host the meeting. Immediately after each meeting, transfer the video to a folder in your official school Google Drive named 'Zoom Recordings' and delete from the device once uploaded.
- Lastly, no video/audio is enabled until there are at least two pupils present in the meeting with the teacher, to avoid the possibility of 1:1 online conversations which are not advised.