The Golden Thread Alliance

ICT and Acceptable Use Policy

Date Reviewed	*Spring 2026*
Next Review Date	*Spring 2028*

This policy has been adopted by all schools within The Golden Thread Alliance

The Golden Thread Alliance

As united as we are different.

Table of Contents

1. Introduction & Aims

Information and communications technology (ICT) is an integral part of the way our schools work, and is a critical resource for pupils, colleagues (including Senior Leadership Teams), Governors, Trustees, volunteers and visitors.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for colleagues, pupils, parents and carers, Governors and Trustees
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, behaviour and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including Governors, Trustees, colleagues, pupils, volunteers, contractors and visitors (including parents and carers).

Breaches of this policy may be dealt with under our:

- People Manual
- Parent and Carer Conduct
- Behaviour Policy
- Suspensions and Permanent Exclusions Policy
- Colleague Disciplinary Procedure
- Safeguarding and Child Protection Policy

2. Relevant Legislation and Guidance

This policy refers to and complies with the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones (mobile and landlines), music players or hardware, software, websites, virtual assistant technology, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including Governors, Trustees, colleagues, pupils, volunteers, contractors and visitors (including parents and carers)
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose agreed by authorised personnel
- **"Authorised personnel":** employees authorised by the school or Trust to perform systems administration and/or monitoring of the ICT facilities

- **"Materials":** files and data created using the ICT facilities, including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See Appendix 6 for a glossary of cybersecurity terminology.

4. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school or Trust, or risks bringing the school or Trust into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community, unless deemed necessary for safeguarding purposes
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school or Trust
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Pupils using AI tools and generative chatbots (such as ChatGPT and Google Bard):

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The schools and Trust reserve the right to amend this list at any time. The Headteacher or any other relevant colleague of the school Senior Leadership Team and/or Trust Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school or Trust's ICT facilities.

4.1 Exceptions from Unacceptable Use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

Approval for such activities would be sought from the Trust CEO by the Headteacher.

Pupils may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example, in ICT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions

Pupils and colleagues who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's and Trust policies on behaviour, safeguarding, dealing with racist incidents, suspensions and permanent exclusions, colleague discipline, colleague code of conduct, parent and carer conduct. Copies of these policies can be found on the school and Trust websites.

5. Colleagues (including Trustees, Governors, Volunteers, and Contractors)

5.1 Access to School ICT Facilities and Materials

The Trust's ICT facilities and services company (Gridserve) manages access to the ICT facilities and materials for colleagues. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Colleagues will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Colleagues who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT service team.

Colleagues and pupils should treat any property belonging to the school or Trust with respect and reasonable care and report any faults or breakages immediately to the Headteacher or line manager. You should not use the Trust's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

5.1.1 Use of Phones and Email

The Trust provides each colleague and governor with an email address.

This email account should be used for work purposes only. Colleagues should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the Trust has provided. Colleagues must not share their personal email addresses with parents, carers and pupils, and must not send any work-related materials using their personal email account.

Colleagues must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to subject access requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Colleagues must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If colleagues receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If colleagues send an email in error that contains the personal information of another person, they must inform the Headteacher or Data Protection Officer immediately and follow our data breach procedure as set out in our Data Protection Policy.

Colleagues must not give their personal phone numbers to parents, carers or pupils. Colleagues must use phones provided by the school to conduct all work-related business where possible. If personal phones are used to contact parents and carers, the colleague's number must be withheld, and parents' and carers' numbers must be deleted from the call log.

School phones must not be used for personal matters.

Colleagues who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The Trust and school record all incoming and outgoing phone conversations.

Callers must be made aware that the conversation is being recorded and the reasons for doing so. Phone conversations are recorded for training and quality purposes.

Use of social messaging apps, including WhatsApp or any other messaging apps, for work-related discussions must remain professional, respectful and consistent with company policies. Messages about colleagues, pupils or Trust business should not include inappropriate, offensive, or speculative comments, nor should they disclose confidential or personal information. Colleagues should avoid discussing other colleagues' sickness, performance, or personal circumstances in informal group chats. Communication sent outside of work, on private devices, or in private groups may still be subject to investigation if it impacts the workplace, breaches confidentiality, or causes offence or harm to others. All colleagues are expected to communicate in a respectful and inclusive manner at all times, regardless of platform.

5.2 Mobile Phone Use

Colleagues (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, when pupils are present. Use of personal mobile phones is restricted to non-contact time, and to areas of the school where pupils are not present (such as designated colleague areas or classrooms when children are at lunch or break, etc.).

There may be circumstances in which it's appropriate for a colleague to have use of their phone during contact time. For instance:

- For emergency contact by their child or their child's school
- In the case of acutely ill dependents or family members
- As part of the lockdown or evacuation procedures

The Headteacher/Line Manager will decide on a case-by-case basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school colleagues can use the school office number as a point of emergency contact.

Colleagues must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil without prior permission from the Headteacher. If it is necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment wherever possible. Colleagues should ensure that correct photo consent is in place for pupils before taking photos.

The school and Trust accepts no responsibility for personal mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while colleagues are travelling to and from school.

5.3 Use of WhatsApp and Similar Messaging Applications

WhatsApp and similar instant messaging applications are not approved school communication systems and must be used only in limited circumstances.

Colleague may use WhatsApp only for internal colleagues communication and operational matters where approved school systems are unavailable. Any use must remain professional, proportionate and necessary.

Colleagues must not:

- Communicate with pupils or former pupils via WhatsApp
- Use WhatsApp to communicate with parents or carers on school matters
- Share personal, sensitive or special category data (including safeguarding, SEN, medical, behaviour or assessment information)
- Share images, videos or audio recordings of pupils
- Use WhatsApp as a substitute for official school communications systems.

Colleagues should be aware that WhatsApp content is stored on personal devise and cannot be centrally monitored or audited. Devices must be secured and any data protection or safeguarding concerns must be reported in line with Trust procedures.

Misuse of WhatsApp may result in disciplinary action in accordance with Trust policies.

5.4 Personal Use

5.4.1 ICT for Personal Use

Colleagues are permitted to occasionally use school ICT facilities and networks for personal use, subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher/Line Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Takes place during break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when pupils are not present
- Does not interfere with their jobs, or prevent other colleagues or pupils from using the facilities for work or educational purposes

Colleagues may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Colleagues should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Colleagues are also permitted to use their personal devices (such as mobile phones, laptops or tablets) in line with the People Manual, Safeguarding and Child Protection policy and this policy.

5.4.2 Personal Social Media Accounts

Colleagues should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

Colleagues must not give their personal contact details to parents and carers or pupils, including connecting through social media and messaging apps.

Colleagues must avoid publicising their contact details on any social media platform or website to avoid unwanted contact by parents and carers or pupils.

The school has guidelines for colleagues on appropriate security settings for Facebook accounts (see Appendix 1).

5.5 Remote Access

We allow colleagues to access the Trust/school's ICT facilities and systems remotely.

This may include:

- Office 365 applications
- Web-based software such as Arbour and CPOMS

Colleagues accessing the Trust/school's ICT facilities and systems remotely must abide by the same rules as those accessing the facilities and materials on-site. Colleagues must be particularly vigilant if they use the school or Trust's ICT facilities outside the school and take precautions such as anti-virus software and system security updates, particularly if using a personal device.

Our ICT systems contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

5.6 School and Trust Social Media Accounts

The schools and Trust have official Facebook, X(Twitter) and Instagram pages, managed by school or Trust colleagues. Colleagues who have not been authorised to manage, or post to, the account must not access, or attempt to access, the account.

The school/Trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times. The school may 'filter and monitor' the use of ICT facilities and networks, in line with Keeping Children Safe in Education (KCSIE) guidance.

Authorised personnel may raise concerns about monitored activity with the school's DSL, in line with KSCIE.

5.7 Monitoring and filtering of the school and Trust's network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, he school and Trust reserve the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised colleagues may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school and Trust monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our Board of Trustees is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Colleagues are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant colleagues, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

At the school level, the designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. This is led and overseen by the Trust Safeguarding Lead and Trust Online Safety Lead.

Where appropriate, colleagues may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

The following ICT facilities may be available to pupils, under the supervision of colleagues:

- Computers, laptops and tablets/iPads,
- Specialist ICT equipment, such as that used for music, design and technology, etc

Pupils may be provided with an account linked to the school's virtual learning environment, such as Office 365 or Google Workspace, which they can access from any device.

Pupils will be taught clear expectations around the appropriate use and care of IT facilities to ensure their safety and to protect the equipment being used. Deliberate failure to follow these expectations may result in a sanction being enforced or use of the equipment being removed.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school/Trust has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation. Details of this can be found in the Online Safety Policy, section 6.3 Examining electronic devices.

6.3 Use of Cameras, Microphones and Recording Tools

Pupils must not use cameras, microphones, audio or video recording functions on any device unless a colleague has given explicit permission. Pupils must not record lessons, colleagues or other pupils, or capture images or audio on school premises without authorisation. Any misuse of recording features will be treated as a breach of this policy.

6.4 Unacceptable use of mobile phones, ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, dealing with racist incidents policy and suspensions and permanent exclusion policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

6.5 Mobile Phones

Pupils are allowed to bring mobile phones to school, but not use them during the school day, and they must be stored with the designated adult within the school. Pupils must adhere to the school's code of conduct and acceptable use agreement for mobile phone use (see Appendix 3 & 4).

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

6.6 Sanctions

If a pupil breaches this policy

- Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006.
- If they are confiscated, a parent or carer will be able to collect the item from school once a meeting has been arranged with a member of the Senior Leadership Team.
- Sanctions for unacceptable use are outlined in the Behaviour policy and Suspension and Exclusion policy

7. Parents and carers

7.1 Access to ICT facilities and materials

Parents and carers do not have access to the school's ICT facilities as a matter of course, other than school communication systems such as Arbor or Class Dojo.

However, parents and carers working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents and carers are granted access in this way, they must abide by this policy as it applies to colleagues.

7.2 Communicating with or about the Trust or school online

We believe it is important to model for pupils how to communicate respectfully with and about others online.

Parents and carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents and carers to sign the agreement in Appendix 2.

7.3 Use of mobile phones by parents and carers, volunteers and visitors

Parents and carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents and carers or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents and carers
- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents and carers or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in this policy.

Parents and carers must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

7.4 Communicating with parents and carers about online activities

Schools will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out at home.

When schools ask pupils to use websites or engage in online activity at home, we will communicate the details of this to parents and carers in the same way that information about homework tasks is shared.

In particular, colleagues will let parents and carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents and carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data Security

The school and Trust are responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Colleagues, pupils, parents and carers, and others who use the school's ICT facilities should use safe computing practices at all times. The Trust and schools will use the government's digital and technology standards in schools and colleges, including the use of;

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school and the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Colleagues are required to regularly change their passwords as and when prompted.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. This includes personal mobile phone security.

Colleagues or pupils who disclose account or password information may face disciplinary action. Parents and carers, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All the school and Trust ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data Protection

All personal data must be processed and stored in line with data protection regulations and the Trust's Data Protection Policy.
The policy can be found on the school and Trust's website.

8.4 Access to facilities and materials

All users of the school/Trust's ICT facilities will have clearly defined access rights to systems, files and devices.

These access rights are managed by Gridserve.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher/DPO immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and completely closed down at the end of each working day.

8.5 Encryption

The Trust ensures that all devices and systems have an appropriate level of encryption.

School and central team colleagues may only use personal devices (including computers and USB drives) to access data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by a Headteacher or Central Leadership Team.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT service provider, Gridserve.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cybersecurity terminology.

The Trust and its schools will:

- Work with Trustees, Governors and the ICT service providers to make sure cyber security is given the time and resources it requires to ensure security
- Provide annual training for colleagues (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure colleagues are aware of its procedures for reporting and responding to cybersecurity incidents
- Investigate whether our ICT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit (such as 360safe) annually, to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data regularly, ideally at least once a day, through the Trust's automatic systems and store these backups on cloud-based backup systems and/or external hard drives that aren't connected to the school network and which can be stored off the school premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider and our ICT service providers.
- Make sure colleagues enable multi-factor authentication where they can, on things like school email accounts
- Make sure ICT providers conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place
- Check that its supply chain is secure, for example, by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the ICT service providers, for example, including how the school will communicate with everyone if communications go down, who will be

contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our Local Authority and local partners to see what it can offer the school and Trust regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

Trust and the school's wireless internet connection are secure. Access to internet content is filtered via Netsweeper. We are aware that filters aren't foolproof. All stakeholders should report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the relevant colleague or Gridserve.

10.1 Pupils

The school and Trust's approach to the use of the internet by pupils includes:
- The use of content filtering and monitoring by Netsweeper
- Pupil phones are not to be connected to the school Wifi
- Supervision by colleagues when pupils access the internet on school devices on the school site
- Netsweeper filtering and monitoring software to be installed on school devices taken offsite by pupils

10.2 Parents, carers, and visitors

Parents, carers, and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:
- Parents and carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Colleagues must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Headteacher, Central leadership team and network providers monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.
This policy will be reviewed every year.

12. Related Policies

This policy should be read alongside the school's policies on:
- Online Safety

- Safeguarding and Child Protection
- Behaviour Policy
- Dealing with Racist Incidents
- Suspensions and Permanent Exclusion
- People Manual
- Data Protection
- Educational Visits Procedure

Appendix 1: Social Media Quick Reference Guide for Colleagues

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other colleagues in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school/trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts on Facebook.
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your Facebook profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if—

A pupil, parent or carer adds you on social media

- In the first instance, ignore and delete the request. Block the user from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- Notify the senior leadership team or the headteacher about what's happening

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or colleague, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

- If the perpetrator is a parent or carer, or other external adult, a senior colleague should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable Use of the Internet: Agreement for Parents and Carers

Acceptable use of the internet: What Parents and Carers Need to Know
Name of parent or carer:
Name of child:
At our school and Trust, we use tools like Class Dojo, Arbor, Office 365, Google Workspace and social media (Facebook, Instagram, X) to share learning and communicate with families.
We want these tools to be safe and positive for everyone.
By signing this agreement, I understand and agree to the following:
How I'll communicate with the school and Trust:

- Be respectful towards colleagues, the school and the Trust at all times
- Be respectful of other parents, carers and children
- Direct any complaints or concerns through the school or Trust's official channels, so they can be dealt with in line with the complaints procedure

What I won't do:

- Use the school or Trust's social media pages or personal social media to complain about or criticise colleagues—I understand this doesn't help the school solve problems.
- Use the school or Trust's social media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school or Trust and speak to the appropriate colleague if I am aware of a specific behaviour issue or incident
- I won't share pictures or videos of children (except my own) unless I have permission from their parent or carer.

I understand that:

- My child has talked about online safety in school and has been taught how to use the internet safely.
- The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people are safe when they use the internet and systems.
- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- The school may monitor what my child does online and will contact me if there are any concerns.

Signed:

Date:

Appendix 3: Acceptable Use Agreement for Older Pupils (KS2)

How I Use the Internet and School Devices

Name of pupil:
I use computers, tablets, and the internet at school to learn, create, and explore.

To help keep everyone safe and happy, I promise to follow these online rules:

- I will ask for permission before using school devices.
- Use only my own login details and not share these with others. If they don't work, I'll tell an adult.
- I'll only do school tasks unless a teacher says I can play or explore something else.
- I'll take care of the devices and tell an adult if something breaks.
- I won't change settings or install things without asking.
- If I make a mistake, I'll ask for help.
- If I see something upsetting or worrying, I will STOP, CLOSE the device, and TELL an adult.
- Check with an adult before clicking links or attachments I'm not sure about.
- I will not use the camera or microphone on my device unless a teacher has told me to.
- I will never record lessons, adults, or other pupils without permission.

I will also:

- Be kind to others online.
- Keep personal information (like my name, address, or password) private.
- Never take or share pictures of anyone without asking them first.
- Never copy other people's work and say it's mine.
- Only use my phone or personal devices at school if I've been given permission.
- Hand in my phone or personal device if asked for safekeeping.

I know adults check what I do online to keep me safe.

We've talked about these rules together and agreed to follow them.

Signed (pupil):
Date:

Appendix 4: Acceptable Use Agreement for Younger Pupils (KS1)

My Computer and Internet Rules at School

Name of pupil:
We use computers, tablets, and the internet to play, learn, and explore. To keep everyone safe and happy, we have some simple rules to follow.

I will:

- Ask my teacher or adult before I use a computer or tablet.
- Only use the apps and websites my teacher says are okay.
- Take care of the devices and tell an adult if something breaks.
- Ask for help if something goes wrong.
- I will only take photos or record if my teacher says it's OK.

If I see something that upsets me:

I will STOP, CLOSE the screen, and TELL an adult straight away.

I will also:

- Be kind online.
- Never share my name, school, or pictures online.
- Only take pictures if everyone says it's okay.

I know that adults at school will check what I'm doing online to make sure I'm following these rules and to keep me safe.

We've talked about these rules together and agreed to follow them.

Signed (pupil):
Date:

Appendix 5: Acceptable Use Agreement for Visitors

Acceptable use of mobile phones, the school's ICT facilities and the internet: agreement for visitors

Name of visitor:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Access, or attempt to access, inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites on school ICT equipment
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or colleagues, or other members of the community
- Access, modify, delete or share data I'm not authorised to access, modify, delete or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (visitor):
Date:

Appendix 6: Glossary of Cybersecurity Terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/ multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

West Hill Primary Academy
Dartford Road,
Dartford, Kent,
DA1 3DZ

01322 296140

hello@golden-thread.org

The Golden Thread Alliance

As united as we are different.