At Weaver Trust, we work to ensure that all in our community believe, belong, and thrive. This policy is informed by our Trust's vision of inspiring all to believe in their own ability to achieve their full potential, both academically and socially. By living by our values of being innovative, responsible and caring, we create powerful learning communities - positively impacting all.

1. Policy Statement

1.1 This notice explains what personal data (information) we hold about you, how we collect it, how we use it, and how we may share it. We are required to give you this information under data protection law.

2. Definitions

Term	Definition
Trust	Is Weaver Trust Limited, Suite 2, Oak Tree Barn, Hatton Lane, Warrington, WA4 4BX and its subsidiary organisations, and clubs, collectively referred to as the 'Trust'
Department for Education (DfE)	Is the government department which deals with education
Local Authority (LA)	is Cheshire West and Chester Council, The Portal, Wellington Road, Ellesmere Port, CH65 0BA or Halton Borough Council, Municipal Building, Kingsway, Widnes, Cheshire, WA8 7QF
Chief Executive Officer (CEO)	Is Annette Williams
Designated Safeguarding Lead (DSL)	Is Annette Williams
Trust Governance and Communications Manager	Is Phil Atkinson
IT Representative	Is Dean Stening
Social Media Representative	Is Becky Coates
Trust Data Protection Officer (DPO)	Is Tru-Digital Protection T/A Tru-Digital Services Ltd, 5 Brayford Square, London, E1 0SG dpo@trudigital.co.uk
Data Controller	Is the Trust for UK data protection law
ICT Facilities	All facilities, systems and services, including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players,

	hardware, software, websites, web applications or services, and any device, system or service that may become available in the future, which is provided as part of the Trust's ICT service
Users	Anyone authorised by the Trust to use the Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
Personal Use	Any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
Authorised Personnel	Employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities
Materials	Files and data created using the Trust's ICT facilities, including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
Social Media Accounts	The Trust uses the following • Facebook • Instagram • X (aka Twitter)
Social Chat Accounts	The Trust uses the following • Facebook Messenger • Whatsapp

3. Introduction

3.1 Information and communications technology (ICT) is an integral part of how our Trust operates, serving as a critical resource for pupils, staff (including the senior leadership team), governors, volunteers, and visitors. It supports teaching and learning, as well as the Trust's pastoral and administrative functions.

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

3.3 This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents/carers and governors

- Establish clear expectations for the way all members of the Trust community engage with each other online
- Support the Trust's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the Trust through the misuse, or attempted misuse, of ICT systems
- Support the Trust in teaching pupils safe and effective internet and ICT use

3.4 This policy covers all users of our Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

3.5 Breaches of this policy may be dealt with under our:

- Disciplinary policy.
- Behaviour policy.
- Staff discipline policy.
- Staff code of conduct.

3.6 This policy must be approved by the governing body and signed by the Headteacher and the Chair of Governors.

4. Relevant Legislation and Guidance

4.1 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 The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- 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 2025
- 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 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

5. Unacceptable Use

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

5.2 Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright.
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the Trust'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.
- Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute.
- Sharing confidential information about the Trust, its pupils, or other members of the Trust community.
- Connecting any device to the Trust's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the Trust's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the Trust's 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 Trust's ICT facilities.
- Causing intentional damage to the Trust's ICT facilities
- Removing, deleting or disposing of the Trust's ICT equipment, systems, programmes or information without permission from authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the Trust.

- Using websites or mechanisms to bypass the Trust's filtering or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.
- Using AI tools and generative chatbots (such as ChatGPT and Google Gemini):
    - 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.

5.3 This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Headteacher or any other delegated member of staff will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's ICT facilities.

5.4 Exceptions from unacceptable use

5.4.1 Where the use of Trust ICT facilities (on the Trust 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.

5.4.2 The following approach is an acceptable use of Artificial Intelligence (AI), for example:

- Pupils may use AI tools and generative chatbots, as identified in the Data Protection Impact Assessment.
- AI can be used as a research tool to help researchers discover new topics and ideas.
- When specifically studying and discussing AI in school work, for example, in IT lessons or art homework about AI-generated images. All AI-generated content must be appropriately attributed.

5.5 Sanctions

5.5.1 Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust's policies:

- Disciplinary policy.
- Behaviour policy.
- Staff discipline policy.
- Staff code of conduct.

5.5.2 We may place sanctions for unacceptable ICT use (for instance, revoking permission to use the Trust's systems).

6. Staff (Including Governors, Volunteers, and Contractors)

6.1 Access to Trust ICT Facilities and Materials

6.1.1 The Trust's IT Representative manages access to the Trust's ICT facilities and materials for Trust staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices

- Access permissions for certain programmes or files

6.1.2 Staff will be provided with unique login/account information and passwords that they must use when accessing the Trust's ICT facilities.

6.1.3 Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Representative.

6.2. Use of Phones and Email

6.2.1 The Trust provides each member of staff with an email address.

6.2.2 This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

6.2.3 All work-related business should be conducted using the email address the Trust has provided.

6.2.4 Staff 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.

6.2.5 Staff 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.

6.2.6 Email messages are required to be disclosed in legal proceedings or in response to 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 disclosure. All email messages should be treated as potentially retrievable.

6.2.7 Staff 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 data is only accessible by the intended recipient.

6.2.8 If staff 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.

6.2.9 If staff send an email in error that contains the personal information of another person, they must inform the DPO, Headteacher and the IT Representative immediately and follow our data breach procedure.

6.2.10 Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the Trust to conduct all work-related business.

6.2.11 Trust phones must not be used for personal matters.

6.2.12 Staff 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.

6.2.13 The Trust can record incoming and outgoing phone conversations.

6.2.14 If you record calls, callers must be informed that their conversation is being recorded and the reasons for doing so. Your Trust's phone system probably has an automated option you can use or adapt. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

6.2.15 Staff who would like to record a phone conversation should speak to an IT Representative.

6.2.16 All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved. For instance, you may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

6.2.17 Call recordings are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as emails and paper documents.

6.3. Personal Use

6.3.1 Staff are permitted to occasionally use Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The IT Representative may withdraw or restrict this permission at any time and at their discretion.

6.3.2 Personal use is permitted provided that such use:

- Does not take place during [contact time/teaching hours/non-break time]
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes

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

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

6.3.5 Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust policy.

6.3.6 Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

6.3.7 Staff should take care to follow the Trust's guidelines on use of social media (see Appendix 1 and social media policy and use of email (see Section 6.2) to protect themselves online and avoid compromising their professional integrity.

6.3.8 Personal social media accounts

6.3.8.1 Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

6.3.8.2 Conversations via social media are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as emails and paper documents.

6.3.8.3 The Trust has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1).

6.3.9 Personal chat accounts

6.3.9.1 Members of staff should make sure their use of chat accounts, either for work or personal purposes, is appropriate at all times.

6.3.9.2 You must not use chat accounts to discuss Trust matters, staff, students, parents or carers.

6.3.9.3 Conversations via chat are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as emails and paper documents. This does include personal accounts.

6.4 Remote Access

6.4.1 We allow staff to access the Trust's ICT facilities and materials remotely. Via either an online portal such as Microsoft 365 or Google Workspace, or using a Virtual Private Network (VPN).

6.4.2 Staff accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the Trust's ICT facilities outside the Trust and must take such precautions as the IT Representative may require against importing viruses or compromising system security.

6.4.3 Our ICT facilities contain confidential information, which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

6.4.4 No unauthorised person must use any equipment provided to you by the Trust or give them access to the Trust's ICT facilities. For the avoidance of doubt, this would include family members, individuals not known to the Trust.

6.5. Trust Social Media Accounts.

6.5.1 The Trust has an official Social Media account, managed by a Social Media Representative. Staff members who have not been authorised to operate or post to the account must not access or attempt to access the account.

6.5.2 The Trust has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage or post to the account must make sure they abide by these guidelines at all times.

6.6. Chat and Messaging Accounts

6.6.1 The Trust has an official Social Chat account, managed by a Social Media Representative. Staff members who have not been authorised to operate or post to the account must not access or attempt to

access the account.

6.6.2 The Trust has guidelines for what may and must not be posted on its social chat accounts. Those who are authorised to manage or post to the account must make sure they abide by these guidelines at all times.

6.7 Monitoring and Filtering of the Trust Network and Use of ICT facilities

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

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

6.7.2 Only authorised IT Representative, Headteacher or DSL may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Pupils and staff who misuse any of the systems listed above may face disciplinary action in line with the Trust's policies:

- Disciplinary policy.
- Behaviour policy.
- Staff discipline policy.
- Staff code of conduct

6.7.3 The Trust monitors ICT use to:

- Obtain information related to the Trust business
- Investigate compliance with Trust policies, procedures and standards
- Ensure effective Trust 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

6.7.4 Our governing board is responsible for making sure that:

- The Trust meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include guidance on how to manage

processes and systems effectively, as well as how to escalate concerns.

- It regularly reviews the effectiveness of the Trust's monitoring and filtering systems.

6.7.5 The Trust's DSL will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

6.7.6 Where appropriate, staff may raise concerns about monitored activity with the Trust's DSL and IT Representative, as applicable.

7. Pupils

7.1 Access to ICT Facilities

7.1.1 ICT facilities are available to pupils, when and under what circumstances. For example:

- Computers and equipment in the Trust's ICT suite are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Pupils will be provided with an account linked to the Trust's virtual learning environment, which they can access from any device by using a URL.

7.2 Search and Deletion

7.2.1 Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the Headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the Trust rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

7.2.2 This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

7.2.3 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from either the Headteacher, DSL or IT Representative.
- Pupils will be informed of the reason for their search, how and where it will take place,

and will be given the opportunity to ask questions about it.

- Seek the pupil's co-operation. If the pupil refuses to co-operate, you should proceed in accordance with the behaviour policy.
- The authorised staff member should:
- Notify the DSL of any searching incidents where there were reasonable grounds to suspect a pupil owned a banned item.
- Involve the DSL without delay if they believe that a search has revealed a safeguarding risk.

7.2.4 Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so If concerned, you can contact the DPO.

7.2.5 When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, and/or
- Undermine the safe environment of the Trust or disrupt teaching, and/or
- Commit an offence

7.2.6 If inappropriate material is found on the device, it is the responsibility of the Headteacher, DSL, or another member of the senior leadership team to determine an appropriate response. If there are images, data, or files on the device that staff reasonably suspect could put a person at risk, they will first consider the appropriate safeguarding measures.

7.2.7 When deciding whether there is a valid reason to erase data or files from a device, consult the DPO who will assess whether the material might be evidence related to a suspected offence. In these cases, they will not delete the material, and the device will be surrendered to the police as soon as reasonably practicable. If the material is not suspected to be evidence in connection with an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

7.2.8 If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Do not view the image
- Do not copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will decide on line with the DfE's latest guidance

on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) latest guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

7.2.9 Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The behaviour policy or search and confiscation policy.
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Trust's complaints procedure.

7.3. Unacceptable Use of ICT and the Internet Outside of School

7.3.1 The school will sanction pupils, in line with the Behavior policy, if a pupil engages in any of the following at any time (even if they are not on Trust 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 Trust's policies or procedures.
- Any illegal conduct, or making 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 or 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 Trust, or risks bringing the Trust into disrepute.
- Sharing confidential information about the Trust, other pupils, or other members of the Trust 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 Trust's ICT facilities.
- Causing intentional damage to the Trust's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without

authorisation

- Using inappropriate or offensive language

7.3.2 If pupils are caught doing any of the above, then Sanctions may apply, which are set out in section 5.2.

8. Parents or Carers

8.1 Access to ICT Facilities and Materials

8.1.1 Parents/carers do not have access to the Trust's ICT facilities as a matter of course.

8.1.2 However, parents/carers working for, or with, the Trust 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 Trust's facilities at the headteacher's discretion.

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

8.2. Communicating with or About the Trust Online

8.2.1 We believe it is vital to model respectful communication for pupils and help them learn how to interact with others online in a respectful manner.

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

8.3. Communicating with Parents/Carers About Pupil Activity

8.3.1 The Trust will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

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

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

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

9. Data Security

9.1 The Trust is responsible for ensuring that it has the appropriate level of security protection and procedures in place to safeguard its systems, staff, and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is periodically reviewed to keep pace with evolving cybercrime technologies.

9.2 Staff, pupils, parents/carers and others who use the Trust's ICT facilities should use safe computing practices at all times. We aim to meet the cybersecurity standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

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

9.3 Passwords

9.3.1 All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

9.3.2 Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

9.3.3 Members of staff or pupils who disclose account or password information may face disciplinary action.

9.3.4 Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

9.3.5 All staff will use the password vault required by the IT Representative to store their passwords securely.

9.3.6 Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

9.4 Software Updates, Firewalls and Anti-Virus Software

9.4.1 All of the Trust's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

9.4.2 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 Trust's ICT facilities.

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

9.5 Data Protection

9.5.1 All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy.

9.6 Access to Facilities and Materials

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

9.6.2 An IT Representative manages these access rights.

9.6.3 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 IT Representative immediately.

9.6.4 Users should always log out of systems and lock their equipment when not in use to prevent any unauthorised access. Equipment and systems should always be logged out of and fully shut down at the end of each working day.

9.7 Encryption

9.7.1 The Trust makes sure that its devices and systems have an appropriate level of encryption.

9.7.2 Sensitive emails should be encrypted if being sent outside the Trust environment.

10. Protection from Cyber Attacks

10.1 Please see the glossary (appendix 6) to help you understand cybersecurity terminology. The Trust will:

- Work with governors and the IT department to make sure cybersecurity is given the time and

resources it needs to make the Trust secure

- Provide annual staff training (and include this training in any induction for new starters, if they join outside of the Trust's yearly training window) on the basics of cyber security, including how to:
  - Check the sender's 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 staff are aware of the procedures for reporting and responding to cybersecurity incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Do not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - Proportionate: The Trust will verify this using a third-party audit (such as 360 degree safe) at least annually, to objectively test that what it has in place is effective.
  - 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 Trust needs to update its software.
  - Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be.
- For on-premise data backup, ensure critical data is regularly saved—ideally at least once a day (it can be automated)—and store these backups in the cloud.
- Make sure staff:
  - Use secure portals or use a virtual private network (VPN) when working from home
  - Enable multi-factor authentication (aka two-factor authentication) where they can, on all critical software accounts
  - Store passwords securely using a password vault.
- Ensure ICT staff conduct regular access reviews to ensure each user in the Trust has the appropriate level of permissions and administrative rights.
- Have a firewall in place that is switched on.
- Ensure its supply chain is secure, for example, by asking suppliers about their business practices and verifying if they hold the Cyber Essentials certification.
- Develop, review and test an incident response plan with the IT department, including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be

reviewed and tested, and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.

11. Internet Access

11.1 The Trust's wireless internet connection is secure, and all traffic to the internet will be filtered, in line with Section 6.7.

11.2 WiFi is provided to support Students and Staff

11.3 Parents/Carers and Visitors

11.3.1 Parents, carers, and visitors to the Trust are not allowed to use the Trust's WiFi unless they have specific authorisation from the Headteacher or IT Representative.

11.3.2 They will only grant authorisation if:

- Parents/carers are working with the Trust in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the Trust's WiFi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

11.3.3 Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Approved by: _____ _____

Chair of Trust **CEO**

Date: _____ _____

Appendix 1 – Facebook Cheat Sheet for Staff

Do not accept friend requests from pupils on social media

1. 10 Rules for School Staff on Facebook

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
- Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional.
- Check your privacy settings regularly.
- Be careful about tagging other staff members in images or posts.
- Don't share anything publicly that you wouldn't be happy showing your pupils
- Don't use social media sites during school hours.
- Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
- 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).
- Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) can find you using this information.
- Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils).

2. 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.
- 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 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

3. What to do if….

3.1 A pupil adds you on social media.

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Recheck your privacy settings, and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the headteacher about what's happening.

3.2 A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to a parent or carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school.
  - Pupils may then have indirect access through their parent or carer's account to anything you post, share, comment on or are tagged in.
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent or carer know that you're doing so.

3.3 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 staff member, our mediation and disciplinary procedures are typically sufficient to address online incidents.
- If the perpetrator is a parent/carer or other external adult, a senior member of staff 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 – Cyber Security Terminology

These key terms will help you to understand the common forms of cyber attack and the measures the Trust 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 (such as 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	Programmes 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 people in an organisation.