Diocese of Norwich Education and Academies Trust

ICT and internet acceptable use policy

Policy Type:	**Trust Policy**
Date Issued by MAT:	**18/03/2026**
Approved By:	**Joint Policy Development Committee**
Approval Date:	**12/03/2026**
Review Date:	**March 2027**
Person Responsible:	**DoNESC Executive Assistant to the CEO/Project Manager**

Our Christian Ethos and Values

All policies within the Diocese of Norwich Education and Academies Trust (hereafter referred to as "the Trust"), whether relating to an individual academy or the whole Trust, will be written and implemented in line with our Christian ethos and values.

We have high ambition for all, and we truly value the wider educational experience.

We walk and talk our Christian values. We put people at the centre of the organisation and want to see them flourish and grow. Our schools are inclusive, welcoming those of all faiths and none.

Overall accountabilities and roles

The Trust has overall accountability for all its academies and staff. Through a Scheme of Delegation it sets out the responsibilities of the Trust, its Executive Officers, the Local Governance Committee and the Principal / Headteacher. The Principal / Headteacher of each academy is responsible for the implementation of all policies of the Trust.

All employees of the Trust are subject to the Trust's policies.

Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 4
4. Unacceptable use 4
5. Staff (including Governors, Trustees, volunteers, and contractors where appropriate) 6
6. Pupils 10
7. Parents/carers 13
8. Data security 13
9. Protection from cyber attacks 15
10. Internet access 16
11. Monitoring and review 16
12. Related policies 16
    Appendix 1: Acceptable use agreement for secondary pupils 18
    Appendix 2: Acceptable use agreement for primary pupils 19
    Appendix 3: Acceptable use agreement for staff, Governors, volunteers and visitors 20
    Appendix 4: Glossary of cyber security terminology 21
    Appendix 5: Sending Personal Data 23

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Trust works, and is a critical resource for pupils, staff, Governors, Trustees, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the Trust.

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

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents/carers, volunteers, contractors, visitors, Governors and Trustees.
- 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 or its academies through the misuse, or attempted misuse, of ICT systems.
- Support the academies in teaching pupils safe and effective internet and ICT use.

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

Breaches of this policy may be dealt with under the Trust Disciplinary Procedures for All Staff, Code of Conduct for Staff and Volunteers or academy Behaviour 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 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
- 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:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or 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, Trustees, 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

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

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).

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 or the academy'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 academy or Trust, or risks bringing the academy or Trust into disrepute.
- Sharing confidential information about the Trust, the academy, its pupils, or other members of the academy and 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 academy or 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 Artificial Intelligence (AI) tools and generative AI (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 Trust reserves the right to amend this list at any time. The Headteacher and Trust 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.

4.1 Exceptions from unacceptable use

Where the use of Trust ICT facilities (on 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 or, where appropriate, CEO's discretion and must be applied for in writing via email to the Headteacher or CEO.

Pupils may use AI tools and generative AI:

- When directed to by a teacher for the purpose of exploring the issues of utilising AI and its potential harm
- When specifically studying and discussing AI in schoolwork and its use has been permitted by a teacher, for example:
    - in IT lessons when there is a course requirement and allowed by the teacher
    - in Art for discussion and work on the benefits and consequences of AI-generated images
- All AI-generated content must be properly attributed.

All users should apply the principles of Data Protection when using AI tools and generative AI.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust Disciplinary Procedures for All Staff, Code of Conduct for Staff and Volunteers or the academy Behaviour Policy.

5. Staff (including Governors, Trustees, volunteers, and contractors where appropriate)

5.1 Access to academy ICT facilities and materials

OfficeXpress (OX) manages access to the Trust's ICT facilities and materials for staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the Trust's ICT facilities and passwords should not be shared.

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 OX - Service Desk support@officexpress.co.uk.

5.1.1 Use of phones and email

The Trust provides each staff member and Trustee with an email address.

This email account should be used for work purposes only.

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

Staff must not share their personal email addresses with parents/carers or pupils and must not send any work-related materials using their personal email account.

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.

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 the purposes of disclosure. All email messages should be treated as potentially retrievable.

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

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.

If a staff member finds or causes a data breach or potential breach, the staff member must follow the Trust's data breach procedures as outlined in the Trust's Data Protection Policy.

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 official work-related business.

Trust phones must not be used for personal matters.

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.

The Trust may be able to record incoming and outgoing phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. The academy's/Trust's phone system may have an automated option which can be used/ adapted.

Where phone conversations are recorded, the purpose for recording must be explained clearly to all parties. For instance:

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

Staff who would like to record a phone conversation should speak to the Headteacher or where appropriate, Trust CEO.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

Requests for recording may be granted by the Headteacher or Trust CEO 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 assessments etc.
- Discussing requests for term time holidays.

5.2 Personal use

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

Personal use is permitted provided that such use:

- Does not take place during contact time/ teaching hours/ non-breaktime.
- 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.

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

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.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the requirements outlined in the Code of Conduct Policy (excerpt below)

Staff and volunteers must only communicate with pupils/students and parents or carers using official Trust systems, and any such communication must be in a professional tone and manner.

Staff and volunteers must ensure that if they bring any personal equipment on to a Trust site there is no inappropriate content on it, and that it is not accessed by pupils/students at any time.

Any data, including images, which belong to the Trust or pupils/students, must only be stored on Trust owned equipment or systems, and must never be uploaded or downloaded to any personal device for any purpose except in a professional capacity by Governors, Trustees and Members.

Personal devices must never be used to take photos or videos of pupils/students, or to make contact with pupils/students, parents or carers in a professional capacity, unless required in an emergency, for example to make phone contact whilst on a trip or visit if the Trust's equipment is not available.

Staff and volunteers should not use personal mobile phones during working hours and phones should be switched off or switched to 'silent mode'. Staff may use personal mobile phones during break periods if they are not on duty and are out of sight of pupils/students.

Staff and volunteers (except Governors, Trustees and Members) must not use their personal email addresses for work-related matters, unless formally authorised by the Headteacher or CEO.

Where staff or volunteers have relationships with pupils/students, parents or carers by way of family connections or appropriate friendships external to the Trust context, they should declare this to the relevant Headteacher, or for colleagues working centrally the HR Director, to ensure that any personal communication is on record and cannot be misconstrued.

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

Staff should take care to follow the Trust's guidelines on use of social media which is outlined in the Staff Code of Conduct Policy and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

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

The SWGFL (South West Grid for Learning) provides social media checklists to guide staff through the settings of their own personal media accounts. Social Media Checklists | SWGfL

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Report the matter to the Designated Safeguarding Lead
- Check your privacy settings again, 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 will 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 Designated Safeguarding Lead or the Headteacher about what is happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other staff members at the school
    - Pupils may then have indirect access through their parent/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/carer know that you are doing so

You are 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 usually sufficient to deal with 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

5.3 Remote access

The Trust allow staff to access the school's ICT facilities and materials remotely.

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.

Our ICT facilities 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. Please refer to the Trust Data Protection policy for more information.

5.4 Academy social media accounts

Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

Academies must always consider the safety implications when using social media with children and young people. Schools must receive the consent of parents/carers or pupils aged 18 and over before posting any identifiable information or images of children and young people on social media. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of ICT facilities.

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. The filtering and

monitoring is provided by Rydal as the Internet Service Provider. SENSO provides the monitoring of keyboard searches.

. This includes, but is not limited to:

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

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

The Trust monitors ICT use in order to:

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

The Trust board is responsible for making sure that:

- The Trust and its academies meet 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 how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the Trust's monitoring and filtering systems

The Academy's Designated Safeguarding Lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the Academy's DSL, Head of Safeguarding and OfficeXpress.

6. Pupils

6.1 Access to ICT facilities

Explain which ICT facilities are available for pupils. (delete/ add as appropriate)

- Computers and equipment in the academy's ICT suite are available to pupils only under the supervision of staff.
- Specialist ICT equipment in the academy's ICT suite are available to pupils
- Specialist ICT equipment, such as that used for music, or design technology, must only be used under the supervision of staff.
- Pupils will be provided with a school account which they can access by using the following URL (insert web address).

6.2 Search and deletion

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 academy behaviour policy as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

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)

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

- Make an assessment of 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 the Headteacher/ Designated Safeguarding Lead/ appropriate member of senior staff.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation, if the pupil refuses to co-operate, you should proceed according to the behaviour policy.
- The authorised staff member should:
- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available within the behaviour policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk.

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.

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 school or disrupt teaching, **and/or**

- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to 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

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:

- **Not** view the image
- **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 make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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 Academy's Behaviour policy.

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Trust Complaints Procedure.

6.3 Unacceptable use of ICT and the internet outside of the Academy

The academy will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on academy 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 academy'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 academy or Trust, or risks bringing the academy or Trust into disrepute.
- Sharing confidential information about the academy or Trust, other pupils, or other members of the academy 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. Parents/carers

7.1 Access to ICT facilities and materials

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

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

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

7.2 Communicating with or about the Academy or Trust online

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

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

We ask parents/carers to follow the same expectations for conduct online as outlined in the Parent, Carer and Visitor Conduct policy.

7.3 Communicating with parents/carers about pupil activity

The Academy will ensure that parents and carers are made aware of any online activity that the children are engaged with via the availability of the curriculum for this area.

When pupils are asked to use websites or engage in online activity, the details of this will be communicated to parents/carers in the same way that information about homework tasks is shared.

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

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

8. Data security

The Trust is responsible for making sure 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 reviewed periodically to keep up with evolving cyber-crime technologies.

Staff, pupils, parents/carers and others who use the Trust's ICT facilities should use safe computing practices at all times. The Trust are working toward meeting the cyber security 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

8.1 Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords that are at least 10 characters long containing letters and numbers are recommended to access school computers, laptops and other electronic devices. Our IT providers use strength checkers to check the suitability of passwords. Staff and pupils are reminded that they should not reuse passwords from other sites.

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

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Passwords should be kept in a secure location and not written down.

8.2 Software updates, firewalls and anti-virus software

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.

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.

Any personal devices using the Trust's or its academies 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 Data Protection Policy.

8.4 Access to facilities and materials

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

These access rights are managed by OfficeXpress.

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 OfficeXpress 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 shut down completely at the end of each working day.

8.5 Encryption

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

Staff may only use personal devices (including computers and USB drives) to access Trust data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher or CEO. Staff should be using Trust approved methods to share files.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by OfficeXpress and staff should be using Trust approved methods for file sharing.

9. Protection from cyber attacks

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

The Trust will:

- Work with OfficeXpress to make sure cyber security is given the time and resources it needs to make the Trust and its Academies secure
- Provide annual training for staff (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 staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT 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**
    - **Multi-layered**
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested.**
- Back up critical data, this should be the 3-2-1 method. The most common method for creating resilient data backups is to follow the '3-2-1' rule; **at least 3 copies, on 2 devices, and 1 offsite**. This should be regularly and ideally once a day (it can be automatic) and store these back-ups on cloud based systems/ external hard drives that are not connected to the school network.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to OfficeXpress.
- Make sure staff:

    - Enable multi-factor authentication where they can, on things like academy email accounts.
    - Store passwords securely.
- Make sure OfficeXpress staff conduct regular access reviews to make sure each user in the Trust has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification.
- Develop, review and test an incident response plan with OfficeXpress including, for example, how the Trust and its academies will communicate with the appropriate parties if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.

10. Internet access

The Academy and Central Office wireless internet connections are secure.

This is a shared responsibility, between Rydal and OfficeXpress. Rydal provide the internet connection with filtering. If the Academy have servers, OfficeXpress will provide security permissions on the folders. Each Academy is responsible for making sure that only the correct people access the Wi-Fi ie the password to the "main Network" isn't shared with guests. If required, the Academy and Trust Central Offices should have a guest Wi-Fi Network. At the Central Office, Trust Central Staff should ensure that only the guest Wi-Fi Network and password is shared with guests if required.

10.2 Parents/carers and visitors

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

The Headteacher will only grant authorisation if:

- Parents/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)

Staff 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 monitors the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Academy.

This policy will be reviewed annually and approved by the Trust Board.

12. Related policies

This policy should be read alongside the Trust and Academy policies including:

- Behaviour Policy
- Code of Conduct for Staff and Volunteers
- Data Protection Policy

- Parent, Carer and Visitor Conduct Policy
- Remote Learning
- Safeguarding and Child Protection Policy
- Staff Disciplinary Policy

Appendix 1: Acceptable use agreement for secondary pupils

Adapt this agreement to reflect your academy's approach.

Acceptable use of the Academy's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

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

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use AI tools and generative AI (such as ChatGPT or Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work

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 a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement for primary pupils

Adapt this agreement to reflect your academy's approach.

Acceptable use of the Academy's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me. • Use them to break school rules • Go on any inappropriate websites. • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms. • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes. • Share my password with others or log in using someone else's name or password • Bully other people • Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement for staff, Governors, volunteers and visitors

Acceptable use of the Academy's ICT facilities and the internet: agreement for staff, Governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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 or chat rooms • 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 staff, or other members of the community. • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, 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 take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will 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 (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Glossary of cyber security 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.

TERM	DEFINITION
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.

Appendix 5: Sending Personal Data

Sending Personal Data

Please use encrypted communications channels when transmitting any personal data over an untrusted network, meaning when it leaves an internal system. This currently means when sharing data between schools and the central team as well as more obviously external contacts. There are 3 main options easily available either integrated with or accessed from our existing IT systems.

Personal data is defined in the UK General Data Protection Regulation (UKGDPR) as:
"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
The UK GDPR also refers to the processing of 'special categories of personal data'. This means personal data about an individual's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

Personal data can also include information relating to criminal convictions and offences.

Pseudonymisation such as using initials instead of a name **does not** render data unidentifiable under the UKGDPR. So any record using initials to identify an individual should be considered personal data.

In addition, if the data you are sharing refers to "identifiable natural persons" other than the data subject, the other person's data **must** be redacted. For example, where an incident report that you wish to share with parents refers to another child involved in the incident, the other child's details and any identifiable information must be redacted.

The table below provides guidance on email encryption tools and how and when to use them.

Tool	Method	Usage
Google/GMail	You can send messages and attachments with Gmail's confidential mode to help protect sensitive information from unauthorised access. You can use confidential mode to set an expiry date for messages or revoke access at any time. Recipients of the confidential message will have options to forward, copy, print and download disabled.	For communications outside the Trust or school, i.e. with parents, other schools and the Local Authority or between schools and Trust. The default attachment size limit for email accounts is often 25 MB – if you are sending a large amount of data e.g. in response to a SAR

	Note: Although confidential mode helps prevent the recipients from accidentally sharing your email, it doesn't prevent recipients from taking screenshots or photos of your messages or attachments.	or to a pupil's new school you may need to use an alternative secure email tool.
Outlook	Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message (the recipient's email address) can decipher the message for reading. You can find the Outlook encryption tool in the Options tab on a draft email. Select encrypt only.	For communications outside the Trust or school, i.e. with parents, other schools and the Local Authority or between schools and Trust. The default attachment size limit for email accounts is often 25 MB – if you are sending a large amount of data e.g. in response to a SAR or to a pupil's new school you may need to use an alternative secure email tool.
We Transfer	Online service to which files can be uploaded and then provides a time-limited (7 days) link only accessible to the intended recipient. www.Wetransfer.com	Large file transfers that it would not be possible to share by email.
GovernorHub	Committees of intended recipients can be created and then access to files of data can be restricted to that committee. The governance team can provide guidance if this method is needed.	**All** communication and file sharing with Governors and Trustees. Can be used for some HR and data protection processes such to share confidential files between existing GovernorHub users.