|  |
| --- |
| **Dale Community Primary**  **and**  **Stonehill Nursery Federation**  **ICT Acceptable Use**  **Policy** |



**Head Teacher: Louise Foster**

**Chair of Governors: Russell Langley**

**Policy Approved by: Governors Behaviour and Safety Committee**

Policy reviewed by: Behaviour and Safety Date: 22 June 2020

Committee

Policy reviewed by: Behaviour and Safety Date: 28 September 2021

Committee

Policy reviewed by: Behaviour and Safety Date: 4 October 2022

Committee

Policy reviewed by: Behaviour and Safety Date: 26 September 2023

Committee

ICT ACCEPTABLE USE

**Introduction and Aims**

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

This policy aims to:

* Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
* Establish clear expectations for the way all members of the school community engage with each other online
* Support the school’s policies on data protection, online safety and safeguarding

Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems

* Support the school in teaching pupils safe and effective internet and ICT use

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

**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 2023
* 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

**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 school’s ICT service
* Users: anyone authorised by the school to use the school’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 school to perform systems administration and/or monitoring of the ICT facilities
* Materials: files and data created using the school’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.

**Unacceptable Use**

The following is considered unacceptable use of the school’s ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see Sanctions below).

* Using the school’s ICT facilities to breach intellectual property rights or copyright
* Using the school’s ICT facilities to bully someone or promote unlawful discrimination
* Breaching the school’s policies or procedures
* Any illegal conduct, or statements which are deemed to be advocating illegal activity
* Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
* Activity which defames or disparages the school, or risks bringing the school into disrepute
* Sharing confidential information about the school, its pupils, or other members of the school community
* Connecting any device to the school’s ICT network without approval from SLT
* Setting up any software, applications or web services on the school’s network without approval by SLT, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
* Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from SLT
* Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
* Causing intentional damage to ICT facilities
* Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by SLT
* Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
* Using inappropriate or offensive language
* Promoting a private business, unless that business is directly related to the school
* Using websites or mechanisms to bypass the school’s filtering mechanisms
* Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

This is not an exhaustive list and the school reserves the right to amend this list at any time.

The Head Teacher and Governing Body will use professional judgement to determine whether any act or behaviour not on the list above is considered to be unacceptable use.

**Exceptions from Unacceptable Use**  
Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the

Head Teacher’s discretion.

**Sanctions**  
Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school’s Behaviour Policy or the Disciplinary and Dismissals Policy.

**Staff Accessing School ICT Facilities and Materials**The school’s IT Manager manages access to the school’s ICT facilities and materials for school staff. That includes, but is not limited to:

* Computers, tablets and other devices
* Access permissions for programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school’s ICT facilities. Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Manager, Mark Berridge.

**Use of Phones and Email**   
The school provides each member of staff 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 school has provided.

Staff must not share their personal email addresses with parents and 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 encrypted 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 staff send an email in error that contains the personal information of another person, they must inform the IT Manager or School Business Manager immediately and follow our data ‘Breach and Compliance Procedure’.

Staff must not give their personal phone numbers to parents or pupils.

Staff must use phones provided by the school to conduct all work-related business unless given permission otherwise by the Senior Leadership Team.

School 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.

Staff must ensure that all personal devices are locked when not in use on site.

**Personal Use**Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Head Teacher, School Business Manager or IT Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

* Does not take place during teaching time
* Does not constitute ‘unacceptable use’
* 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 school’s ICT facilities to store personal non-work-related information or materials (such as documents, music, videos, or photos).

Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities.

Where breaches of this policy are found, disciplinary action may be taken.

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 could see them.

Staff should take care to follow the school’s guidelines on social media and email use to protect themselves online and avoid compromising their professional integrity.

**Personal Social Media Accounts**  
Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. The school has guidelines for staff on appropriate security settings for Facebook accounts (see document: ‘Social Media Guidance for the School Workforce’).

**Remote Access**We allow staff to access the school’s ICT facilities and materials remotely. The network is managed by Link ICT; access is password protected and data transfers are encrypted.

Staff accessing the school’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 school’s ICT facilities outside the school. 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, which can be found on our school website: [www.dale.derby.sch.uk](http://www.dale.derby.sch.uk)

**School Social Media Accounts**  
The school has a twitter account that is managed on behalf of school by the Sports Team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

**Monitoring and filtering of 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 school 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
* User activity/access logs
* Any other electronic communications.

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

The school monitors ICT use in order to:

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

Our governing board is responsible for making sure that:

* The school 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 how to manage the processes and systems effectively and how to escalate concerns
* It regularly reviews the effectiveness of the school’s monitoring and filtering systems

The school’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 school’s DSL and ICT manager, as appropriate.

**Pupils Accessing School ICT Facilities and Materials**

* Computers and tablets are available to pupils under the supervision of staff
* Pupils will have access to software account(s) to support their learning,

e.g. TT Rockstars.

**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 school rules 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
* 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 your 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.
* 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 headteacher 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
* Our behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils’ devices will be dealt with through the school complaints procedure.

**Unacceptable use of ICT and the Internet outside of School**  
The school 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 school premises):

* Using ICT or the internet to breach intellectual property rights or copyright
* Using ICT or the internet to bully someone, or to promote unlawful discrimination
* Breaching the school’s policies or procedures
* Any illegal conduct, or statements which are deemed to be advocating illegal activity
* Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
* Consensual 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 school
* Sharing confidential information about the school, other pupils, or staff
* Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
* Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
* Causing intentional damage to ICT facilities or materials
* Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
* Using inappropriate or offensive language.

**Parents Access to ICT Facilities and Materials**

Parents do not have access to the school’s ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or employee) may be granted an appropriate level of access or be permitted to use the school’s facilities at the Head Teacher’s discretion. Where parents are granted access in this way, they must abide by this policy as it applies to staff.

**Communicating with or about the School Online**We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

**Data Security**The school 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 school’s ICT facilities should use safe computing practices at all times. We aim to meet 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

**Passwords**  
All users of the school’s ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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 or volunteers who disclose account or password information may have their access rights revoked.

Passwords will be required to be updated every 12 weeks and all employee devices and email accounts will request this automatically.

**Software Updates, Firewalls, and Anti-virus software**  
All of the school’s ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

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

Any personal devices using the school’s network must also be configured in this way.

**Data Protection**  
All personal data must be processed and stored in line with data protection regulations and the school’s data protection policy, which can be found on our school website.

**Access to Facilities and Materials**   
All users of the school’s ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by our IT Manager.

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 Manager 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 closed down completely at the end of each working day.

**Encryption**  
The school ensures that its devices and systems have an appropriate level of encryption.

School Staff must use School provided devices whenever they can.  If School devices cannot be used, personal devices can be used but they must be secure, passwords must not be saved or remembered and in no instance can any sensitive data be downloaded or saved to the device.  Remote Access can be used on any device.

**Protection from cyber attacks**

The school will:

* Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
* 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: the school will verify this using a third-party audit (such as 360 degree safe), 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 school needs to update its software
* Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be
* Immediate back up of critical data offsite
* Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department
* Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
* Have a firewall in place that is switched on

**Internet Access**  
The school wireless internet connection is secured. Filters are in place to protect pupils and staff from inappropriate online materials. Please be aware that these are not fool-proof and that you must report anything that is a cause for concern to the IT Manager and a member of the Senior Leadership Team immediately.

Staff may request access to blocked sites if the requirement is of a legitimate school interest. No member of staff is given access to the WIFI password. Personal devices can be handed to the IT Manager, who will enter/store the password on each individual device.

**Pupils and Parents**No pupils or parents will be given personal access to the school WIFI network, unless otherwise granted by the Head Teacher.

**Monitoring and Review**

The Head Teacher and IT Manager will monitor the implementation of this policy and it will be reviewed annually by the school’s Governing Body.

Appendix 1: Facebook cheat sheet for staff

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

2. Change your profile picture to something unidentifiable, or if you don’t, make sure that the image is professional

3. Check your privacy settings regularly

4. Be careful about tagging other staff members in images or posts

5. Don’t share anything publicly that you wouldn’t be happy showing your pupils

6. Don’t use social media sites during school hours

7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there

8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)

9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

10. 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)

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

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
* 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’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

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 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