FLOURISH at Dale and Stonehill

A SCHOOL FOR
Creating Opportunity
& Embracing Innovation
to nurture EACH and
EVERY INDIVIDUAL

Dale Community Primary and Stonehill Nursery Federation

Electronic Communications Policy

Head Teacher:	**Louise Foster**
Chair of Governors:	**Diane Williams**
Policy Approved by:	**Governors Behaviour and Safety Committee**

Policy reviewed by:	Governors Behaviour and Safety Committee	Date: 13 March 2018
Policy reviewed by:	Governors Behaviour and Safety Committee	Date: 23 October 2018
Policy reviewed by:	Governors Behaviour and Safety Committee	Date: 16 June 2020
Policy reviewed by:	Governors Behaviour and Safety Committee	Date: 28 September 2021

ELECTRONIC COMMUNICATIONS

1. Introduction

Dale Community Primary School and Stonehill Nursery School have a range of E-communication systems in place including – email, Internet, Intranet, mobile and landline telephones. These enable us to provide:

- Effective and efficient services to children, parents and other stakeholders.
- Effective communication between staff, children, parents and other stakeholders.
- Flexible and reliable communication channels to allow convenient and far-reaching access to services.

It is important that these systems are used and managed effectively in order to maximise their benefits. However, we also recognise that people lead complex and busy lives and greater flexibility around the use of the communication system at work, e.g. to address personal matters, will help to support staff work-life balance needs.

This policy sets out the expectations of you when using any form of electronic communication, including but not limited to, telephone, email, Internet and Intranet.

This policy sets out:

- Our expectations of you when using e-communications systems.
- Monitoring arrangements.
- The law surrounding electronic communications.
- Good practice guidance.

2. Aims

This policy aims to:

- Set out the expectations of all users of the communication systems, including email, Internet, Intranet and telephones.
- Provide a mechanism that maintains and promotes effective, consistent and legal use of electronic communication.
- Establish and support a balance between protecting the school's interests and respecting your right to carry out your duties with regard for privacy.
- Support your development and work-life balance by allowing reasonable and appropriate personal use of the school's e-communications systems.

3. Scope

The policy applies to the use of equipment, systems and/or networks belonging to or accessed by the school and the use of wireless networks. It covers:

- Staff of the school.
- All other people acting for, or on behalf of, any of the above, including those undertaking activities on an unpaid basis, e.g. work experience or shadowing.

The policy applies to the use of school systems, equipment which is owned by the school and/or networks, at any time during and outside work hours whether on school premises or working at remote locations including home.

4. Protocol

This protocol sets out the minimum expectations when using the e-communication systems however, it is not exclusive or exhaustive. Failure to comply with these requirements may be considered abuse or misuse of e-communications systems.

Passwords and login details must remain confidential.

Access privileges to the electronic systems are granted where appropriate to allow you to perform your work effectively. Administrative privileges are restricted and you must not use or attempt to use these to:

- Install software unless specifically authorised to do so.
- Introduce viruses or other malicious software.

E-communication systems must not be used to:

- Store, send or distribute messages or material which may be perceived by the recipient as:
    - Aggression, threats, abuse or obscenities.
    - Sexually suggestive.
    - Defamatory.
    - Sexually explicit.
    - Discriminatory – whether it be comments, remarks or jokes.
    - Material which the sender knows, or ought to have known, would cause offence to others.
    - Act in a way which contravenes other policies or the law or is likely to bring the school into disrepute.
    - Disclose sensitive information or personal data to unapproved persons or organisations.
    - Intentionally access or download any material containing sexual, discriminatory, offensive or illegal material.
    - Participate in online gambling including lotteries.
    - Participate in online auctions unless authorised to do so for work-related matters.
    - Originate or participate in email chain letters or similar types of communication.
    - Participate in chat rooms/forums unless it is work-related or for professional development purposes.

If you accidently access inappropriate material on the Intranet or by email, disconnect and immediately and inform your manager.

Occasional appropriate and reasonable personal use of email, the Internet and IT equipment is permitted, provided use of the school systems:

- Is restricted to your own time and outside core hours.
- Does not interfere with the performance of duties.
- Does not adversely impact on the performance of the school's e-communication systems or the network.

- Does not involve storing private information or information/data not connected to normal duties.
- Is not for the purpose of furthering outside business interests.
- Does not contravene the requirements of the school's policies or the law.

Remember that misuse of the e-communication systems belonging to, or associated with, the school may breach policies and/or the law and may lead to civil, criminal or disciplinary action including dismissal.

5. Monitoring and recording of the E-communication Systems

Authorised staff of the school's ICT providers may be at any time monitor the use of the e-communications systems.

The use of all e-communications systems particularly email and the Internet is subject to recording in order to detect and deal with abuse of the systems, fault detections and so on. In some cases, monitoring (i.e. real-time observation etc.) of systems may also take place where necessary. Authorised staff will not, without reasonable cause, examine any private material that is discovered.

Personal data should not be stored on the network and you should not expect 'privacy' in relation to accessing websites, personal email correspondence, personal documents stored on school computers or networks or messages sent via the Internet, as these, in principal, are subject to the same checking procedures applied to business related access and email correspondence.

6. Communications and the Law

As well as being bound by the requirements of this policy, you are bound by restrictions under the law. Listed below are the key current legislative regulations that relate to electronic communications:

- General Data Protection Regulation 2018.
- Human Rights Act 1998.
- Regulation of Investigatory powers Act (RIPA).
- Section 160 Criminal Justice Act 1998.
- Computer Misuse Act 1990.

7. Communication of the Policy

New starters will be asked to sign to confirm that they have read and understood the E-Communications Policy.

Particular emphasis will be placed on ensuring that all e-communication users are aware of:

- What e-communication systems may/may not be used for.
- What is considered misuse or abuse.
- What constitutes offensive or inappropriate material as set out in section 4.
- The type of action that is likely to bring the school into disrepute.
- Individuals' responsibilities relating to the use of their own user login and password.

We do not routinely activate email or intranet accounts for temporary staff, including those on temporary contracts, agency workers, unpaid workers or volunteers and consultants. Those who do not use e-communications systems will be asked to confirm that they have read and understood the E-Communications Policy before their IT account is activated.

The policy will be reviewed regularly.

8. Good Practice Guidance

The Internet

The Internet is a source of a great deal of useful information however, it also contains material that is offensive and /or illegal. The schools have a 'Firewall' and other systems that help to protect against viruses and hackers, as well as software which blocks access to inappropriate websites. The content of the Internet changes rapidly so the software will not detect all inappropriate sites.

Do:

- Limit personal use of the Internet to reasonable levels and own time.
- Take advice from line managers before downloading large files or sending large amounts of data via a web-link. To avoid adverse impact on the performance of the systems, these transactions can be scheduled for off-peak times.
- Represent yourself honestly and accurately, including your role in school when using the Internet to participate in social networking.
- If you accidentally access inappropriate material including unexpected 'pop-ups' disconnect immediately and inform your line manager.

Do not:

- Access or download material which is offensive, sexually explicit, discriminatory or illegal.
- Use the Internet for personal use during core work time even if it is minimised on the screen.
- Use systems to participate in online gambling or online auctions unless authorised to do so for work-related matters.
- Download music or video files unless for school purposes.
- Use 'peer to peer' or other file sharing services except where authorised to do so.

Email

Take care when using email to ensure that the language and tone cannot be misinterpreted and that the content is appropriate and accurate. Wherever possible, take steps to reduce the risk of introducing virus infection via email by permanently deleting without opening any of the following:

- Messages or email attachments from unknown sources.
- Unsolicited emails.
- Emails without a subject heading or with a subject heading which looks suspicious.

Concerns that a virus may have entered the system should be reported to the school's IT Technician.

Do:

- Limit personal use of email to reasonable levels and your own time.
- Ensure that your messages are relevant and appropriate to targeted recipients. Do not use 'blanket' or 'all- user' emails.
- Delete messages that are no longer needed as soon as possible.
- Save important emails e.g. as text documents in Word.
- Try to answer emails quickly, politely and professionally.
- Beware of 'email rage'. An email is quick and easy to use and can encourage ill-considered and even offensive messages. Include a subject heading in every email so that the person receiving it knows what it is about.
- Type emails carefully making sure that grammar and spelling are correct. An email is just like a letter and you can expect it to have the same effect.
- Remember that emails have the same legal status as letters and need wording with care.
- Use plain text email messages. This means smaller electronic message sizes and reduces some virus risks.
- Inform management immediately if you receive or see any offensive or sexually explicit material on the Intranet or email messages at work.
- Use your school email address for school business and your personal email address for private communications.

Do not:

- Use email to circulate material which is offensive, illegal, discriminatory or sexually explicit.
- Use email as a substitute for good verbal communication.
- Use words in CAPITAL letters; this can be seen as shouting in an email.
- Send personal information or confidential or sensitive material using external email as it may be accessed unlawfully. This may include bulk forwarding of emails to your own external account.
- Originate or participate in email chain letters or messages including seasonal greetings etc.
- Use the school email to distribute material of a party political nature.
- Expect to receive a response to emails outside of normal working hours.

<u>Social Media</u>

Social networking websites provide an opportunity for people to communicate 'en-masse' and share ideas regardless of geographic distance. Sites such as Facebook, Twitter and Linkedin can serve as a learning tool where training videos and other materials are easily accessible to students in a user-friendly and engaging way. They can also be a useful tool for schools to get key messages out to their community and the wider public.

Other key benefits include:

- Users have a huge degree of control to post comments, photos and/or videos at any time of day.
- Interaction is instant and minute-by-minute.

- Users who have common interests or experiences can connect.
- Communications can be organised locally, regionally, nationally and globally.
- Communication reaches across socially diverse groups.

However, the open nature of the Internet means that social networking sites can leave professionals such as teachers and school support staff vulnerable if they fail to observe a few simple precautions. The following guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position.

School Text Service
Staff who use the school text service to parents and guardians e.g. for children who are attending an overnight residential, must ensure that the texts they send are factual and represent the school in a positive manner.

Privacy

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly.
- Do not, under any circumstances, accept friend requests from a person you believe to be either a parent or a pupil at the school either past or present. The exception to this is if an employee's own child(ren) attend(s) the school or if close friends have children at the school. In these circumstances, it is accepted that communication can take place and that images of their own children and their friends when at parties or such similar personal events can be posted. Care should be taken to ensure the suitability of the images and to use the appropriate security settings. Images should not be posted in relation to the school.

Privacy Setting recommended security level
As a minimum, school recommends the 'Friends only' setting for the following:

- Send you messages
- See your friend list
- See your education and work
- See your current city and hometown
- See your likes, activities and other connections
- Your status, photos and posts
- Bio and favourite quotations
- Family and relationships
- Photos and videos you're tagged in
- Religious and political views
- Birthday
- Permission to comment on your posts
- Places you check in to
- Contact information

Other security recommendations are:

- Always make sure that you log out of Facebook after using it. Your account can be hacked by others if you remain logged in, even if you quit your browser and/or switch the PC/device off. Similarly, Facebook's instant chat facility catches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click 'Clear Chat History' in the chat window).

- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see (or don't post it in the first place!)
- Consider changing your name of Facebook, e.g. do not use your last name.

Conduct on Social Networking Sites

- Do not make discouraging remarks about your employer/colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Act in accordance with the school's E-Communications Policy and any specific guidance on the use of social networking sites.
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online, you should contact them and the site to have the material removed.
- Parents and pupils may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.
- If you have any concerns about information on your social networking site or if you are the victim of cyber-bullying, you should contact the Senior Leadership Team or your Trade Union representative immediately.
- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access your bank and credit card information.
- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click 'Privacy Settings', under 'Applications and Websites' click 'edit your settings'. Scroll down to 'instant personalisation' and make sure the checkbox for 'enable instant personalisation on partner websites' is unchecked.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.