# Email and Internet Policy

| | |
|---|---|
| **Policy owner** | RSSKL - Principal |
| **Policy lead** | Designated Safeguarding Lead |
| **Audience** | All staff and volunteers, pupils and parents of pupils |
| **Legislation and regulation** | Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Telecommunications Regulations 2000, Employment Practices Data Protection Code |
| **Formally endorsed by** | SMTand the Board of Trustees |
| **Endorsement date** | ***11.09.17*** |
| **Next review** | |

## 1 Introduction

1.1 The purpose of this policy is to set out general rules about email and internet usage for staff and volunteers in the course of carrying out their duties at Rudolf Steiner School Kings Langley (RSSKL).

1.2 The RSSKL owns any communications sent via email or stored on RSSKL equipment. SMT and other authorised employees have the right to access any material in emails or on RSSKL equipment at any time and electronic communications, storage and access should not be considered 'private' if it is created or stored at work or on RSSKL equipment.

1.3 Email and internet access is provided to authorised users as a school communication tool for appropriate internal and external work uses. The email and intranet systems are owned solely by the RSSKL.

1.4 Information contained in the system will be treated just like other RSSKL school records, files, electronic records, documents, materials and equipment. Prohibited uses of email are detailed below at 3.8.

1.5 Authorised users must take particular care not to disseminate confidential information about the RSSKL to unauthorised users.

1.6 All users are required to adhere to all the guidelines in this document and should note that any breaches of these may lead to disciplinary action. Serious breaches may constitute gross misconduct and lead to summary dismissal.

## 2 Responsibilities

2.1 Authorised Users:

- should read and adhere to this policy and guidance
- should notify their manager, IT or HR (as appropriate) of any breaches of this policy
- have a duty to ensure that their use of the internet is reasonable and complies with current legislation
- must recognise that internet and email access is not provided for personal use during work time

2.2 SMT:

- should ensure that their authorised users understand this policy
- should ensure IT is informed when access is required for a new member of staff or when access needs to be disabled when a member of staff leaves
- should cooperate with any investigation into system use and misuse

2.3 IT:

- is responsible for providing and removing access under instruction from managers
- provide assistance for any investigation into system use and misuse

## 3 Guidance

3.1 **Email use:** The following rules aim to raise basic awareness, protect the RSSKL's reputation, safeguard sensitive information, encourage best practice and ensure that authorised users take care when sending emails:

- use must have a direct and legitimate school purpose unless specific authority for other use is given
- staff are expected to check their email on a regular basis in accordance with their role

- when an email is received from a parent, an acknowledgement should be sent and, depending on the requirement, a reply should be sent within seven days

- if an email received from a parent is perceived as rude, abusive, bullying or in any way inappropriate do not reply but seek advice and guidance from a member of SMT

- staff must use an RSSKL email account to communicate with parents or upper school pupils

- all group emails to parents must be sent via Schoolcomms (guidelines for using Schoolcomms are available) and agreed by a member of SMT.

- if a parent requests to send out an email via Schoolcomms the message must be checked for appropriateness and must refer to, or relate to school business. Once approved by SMT it can be passed to the school office for sending out

- emails should be written as professionally as a letter, incorrect or improper statements can give rise to personal and organisational liability in the same way as the contents of letters

- emails should be regarded as published information and may be disclosable should a data subject access request be made, or in the course of legal proceedings

- abrupt and inappropriate use of language can be interpreted as bullying in tone and possible offence to others, inappropriate use of capital letters, underlining, and use of bold, exclamation/question marks can often be interpreted as aggressive shouting

- confidentiality can be guaranteed within the schools system and processes however users should be aware that email and the internet can never be considered entirely secure, as both relies on public networks that are outside the school's control and therefore emails can be misdirected by an error in the message routing process, or by the sender

- emails should use children's intials in the header, NOT names

3.2 **Pupil email use:**

- All upper school pupils are provided with a school email address to use

- Email for upper school pupils is only to be used for school based activities

- If inappropriate use is suspected the school reserves the right to check content of a pupil's mailbox (see section on Monitoring at 3.12)

- Teachers may use a pupil's school email address as a method of contacting pupils

3.3 **Parent email use:**

- Parents needing to contact a class teacher must only use the teacher's RSSKL email account. A teacher will not respond to an email sent to their personal email address

- Parents will receive an acknowledgement to an email and should receive a reply within seven days depending on the requirement

- Any communication with teachers and the school must be done in a polite and professional manner. The school reserves the right not to reply, other than in way of an explanation, to any communications deemed rude, abusive, bullying or in any way inappropriate.

- The class contact will ask for the contact details of other parents although no one is compelled to supply them. The school will only give out contact details with the written consent of the individual.

- The Schoolcomms system can be used to communicate to a wider group of people beyond those of a class. The message will be checked by a member of staff for appropriateness and must refer to, or relate to school business. Once approved it will be passed to the school office for sending out

3.4 **Email security:** Security of email, confidential messages, disclaimers and user passwords must take the following in to account:

- internal messages meant only for internal authorised users are not sent to external sources without prior permission

- passwords should not be revealed to anyone, the only exception is if you have clearly established that IT is making the request

3.5 **Leavers process:** When a member of staff is leaving the RSSKL, their manager must ensure that they make appropriate arrangements to handover relevant information during the notice period.

3.6 SMT will inform IT of any leavers and the leaving date. IT will remove access to the network and email account at 5 pm on their last day through an automated process. The email account will remain disabled for 30 days and can be re-enabled at any point during this 30 day period. After 30 days the account will be deleted but can still be accessed for 30 more days through Microsoft. After this period the account and all information contained will not be recoverable.

3.7 It is the relevant member of SMT's responsibility to inform IT if the email account should be assigned to an authorised member of staff on the day that the employee member leaves or that the data from the email account should be saved for a period of time in order to capture certain data before it is deleted.

3.8 **Prohibited use of email:** Prohibited use of the email system includes the following specific examples; however this list is not exhaustive:

- using personal email to communicate with parents or upper school pupils
- sending copies of documents in violation of copyright laws or licensing agreements
- sending confidential information or data to persons not authorised to receive it, either within or outside the school
- solicitation of any type, except for RSSKL sanctioned activities
- excessive use of the email system for non-work related emails
- send or forward mailing lists, chain mail, cartoons, jokes, or gossip
- sending or forwarding emails or distributing, disseminating or storing images, texts or materials that might be considered to be discriminatory, obscene, libellous, derogatory or excessively personal, whether intended to be serious or humorous
- breaking into the school's or any other organisations' systems or unauthorised use of a password or mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-school related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste effort or networked resources
- introducing any form of computer virus or malware into the organisation network
- agreeing to terms, entering into contractual commitments, or making representations by email unless appropriate authority has been obtained
- sending messages from another user's computer, or under an assumed name unless specifically authorised
- unless special provision has been pre-agreed users should only read their own emails

If in doubt whether potential email usage would breach the rules of usage then users should seek the advice of SMT beforehand. Users cannot disclaim responsibility for failure to adhere to these restrictions.

3.9 **Use of the internet:** If used properly the internet is recognised by the school as a powerful, positive, and highly useful tool. Using the internet for personal use is a privilege. It is permitted subject to certain conditions, which are set out below. The RSSKL reserves the right to monitor the use of the internet, including social media and networking sites. For more information please see section on monitoring.

It also reserves the right to withdraw use of the internet or amend the scope of use at any time. The following conditions must be met for personal internet usage to continue:

- in providing this facility the RSSKL needs to ensure that the system is properly managed and authorised users also have a duty to ensure that their use of the internet is reasonable and complies with current legislation
- authorised users must maintain a diligent and professional working environment and recognise that the internet it is not provided for personal use during work time, any personal use must be minimal and take place substantially out of normal working hours (that is during the usual lunch hour or before/after work hours)
- users should not create unnecessary business risks to the organisation by their misuse of the internet
- the internet is a public forum and it should not be assumed that entries on any website will remain private
- employees must be security conscious and should take steps to ensure that no information is made available on the internet that could provide a person with unauthorised access to the RSSKL or any confidential information

3.10 **Use of social media and networking sites:** Social media is a valuable tool for the RSSKL and although its benefits are recognised, the following rules aim to raise basic awareness, protect the school's reputation, safeguard sensitive information, encourage best practice and encourage users to take care:

- authorised users should only use social media and networking sites during working hours for work related purposes
- any personal use must be minimal and take place out of normal working hours (that is during a lunch hour/before/after work hours)
- employees who use social media as part of their job and those who discuss their work via social media and networking sites in a personal capacity should use the same safeguards as they would with any other form of communication about the organisation in the public sphere and any communications must not:
    - bring the school into disrepute, for example by criticising or arguing with colleagues, making defamatory comments about individuals or other organisations or groups, or by visiting sites, which contain inappropriate content
    - breach confidentiality, for example by revealing confidential information or information owned by the school, discussing the school's internal workings that have not been communicated to the public

- breach copyright, for example by using someone else's images or written content without permission, failing to give acknowledgement where permission has been given to reproduce something

- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age using social media to bully another individual (such as an employee of the school), posting images that are discriminatory or offensive (or links to such content)

3.11 **Personal use of social media and networking sites:** it is recognised that members of staff may use social media and networking sites such as Facebook, Twitter and Instagram in their private lives but with this use comes responsibilities linked to being employed within a school:

- Staff should consider making their personal social media pages private and only accessible to invited friends and relatives. They should be aware of inviting or having parents as friends on their personal social media pages

- Staff must decline any contact requests they receive from pupils to their personal social media pages

- Staff must remove any friends or followers who are pupils to their personal social media pages

- Staff must not place any images of school events or school life on their personal social media pages

- Staff must not discuss school related issues on their personal social media pages

3.12 **Prohibited use of the internet:** The following list, which is not exhaustive, shows uses of the internet that are prohibited by the RSSKL at all times:

- gambling

- using the internet, including social media sites for non-work purposes during normal working hours (that is outside a lunch hour or before/after work hours)

- visiting internet sites that contain pornographic, obscene, hateful or illegal material

- downloading, storing, distributing, editing or recording of any kind of sexually explicit image or document

- conducting political activities

- downloading images, music, or videos unless there is an explicit business-related use for the material that has been agreed with the appropriate line manager
- using the computer to perpetrate any form of fraud, or software, film or music piracy (any authorised user who downloads materials in contravention of copyright laws (piracy) will be liable to pay any fine as a result of their action
- using the internet to send offensive or harassing material to other users
- hacking into unauthorised areas
- creating or transmitting defamatory material
- undertaking deliberate activities that waste RSSKL effort or networked resources
- introducing any form of computer virus into the organisations network

The RSSKL reserves the right to restrict access to other sites should they be found to be incompatible with reasonable usage.

3.13 **Personal use of email and the internet:** RSSKL policy is that personal use is a privilege, not a right. The incidental use of its internet, email and telephone systems for personal use is permitted subject to certain conditions set out below. The policy is dependent upon it not being abused or overused, and we reserve the right to withdraw our permission or amend the scope of this policy at any time. The following conditions must be met for personal usage to continue:

- personal use must be minimal and take place substantially out of normal working hours (that is during a lunch hour/before/after work hours)
- personal emails must be labelled “personal” in the subject header
- use must not interfere with school commitments
- use must comply with the RSSKLs’ policies and procedures, including this policy and guidance, the equality and diversity policy, bullying and harassment policy, data protection policy, and disciplinary procedure

3.14 **Monitoring:** The RSSKL systems provide the capability to monitor telephone, email, voicemail, internet, and other communications traffic. For business reasons and in order to perform legal obligations as an employer and a school, use of all our systems and any personal use of them, may be monitored. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for business purposes. The purposes include establishing facts, ascertaining compliance with regulations and codes of practice, ascertaining standards which have or should be achieved by users, determining whether communications are relevant to the school’s business or activities and for preventing or detecting crime.

The RSSKL reserves the right to retrieve the contents and messages or check searches which have been made on the internet for the following purposes:

- to monitor whether the use of the email system or the internet is legitimate and in accordance with RSSKL policy

- to find lost messages or to retrieve messages lost due to computer loss
- to assist in the investigation of wrongful acts
- to comply with any legal obligation
- users of the internet are reminded that web browsers leave “footprints” providing a trail of all site visits and these will be reviewed where reasonable causes for concern over usage arises or subject access requests

3.15 **Handheld devices and laptops:** These business tools remain the property of the RSSKL at all times and may be withdrawn if there is evidence that they have been misused. The following conditions must be met for usage to continue:

- they are provided for work-related purposes to communicate effectively on matters of RSSKL business
- internet usage should follow guidance set out in this document
- although employees are expected to use these tools to carry out RSSKL business efficiently, this does not mean they are expected to be “on-call” at all times and employees have the right to maintain a reasonable work-life balance
- employees are expected to raise any concerns with their manager in the first instance and managers are expected to pick up any concerns where employees are frequently using these tools outside their normal working arrangements
- when attending meetings, other business should not be conducted via these tools at the same time
- mobile device / laptop must be kept secure at all times, especially when travelling
- passwords must be used to secure access to data kept on such equipment in the event that the tool is lost or stolen
- basic safety rules should be observed when using such equipment, such as not using or displaying it in obviously isolated or dangerous areas, or leaving it unattended in a parked car
- please be aware that if using equipment in a public environment then documents may be visible to members of the public
- devices should be encrypted

3.16 **Storage of data being used off premises:** has an obligation to ensure that confidential data is securely stored in accordance with the Data Protection Act:

- storage of RSSKL information should not be excessive and should only relate to information necessary for the operation of the role undertaken

- critical information (i.e. personal identifiable as well as commercial sensitive information) should be stored on the RSSKL network only

- USB memory sticks should be a short term mechanism for transferring data and should not be used to store data on a permanent basis.  devices should be encrypted

- authorised users who are storing information outside of normal business premises must have their line manager's permission to do so and must take proper care of it and ensure its security at all times e.g. not left unattended, transmitted/copied to other people

- at the end of their employment staff are not permitted to hold RSSKL information

- any removable media devices must be returned to your manager and any other information deleted as appropriate

- any loss of RSSKL information should be reported immediately to your manager in accordance with information security incidents specified within the information security policy

- all information security events and suspected weaknesses are to be reported to the IT immediately, all of these events shall be investigated to establish their cause and impacts with a view to avoiding similar events