Rosebank School

Listening, Responding, Learning

POLICY FOR ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION, INCLUDING THE INTERNET

DATE OF THIS POLICY:	June 2024
Ratified by Governors:	June 2024
Frequency of update:	Every 3 years
Due for revision:	June 2027
Person responsible:	Natasha Tompkins

The next revision date is:

Review Date	Changes Made	By Whom
June 2024	Information regarding smart watches	Natasha Tompkins

ROSEBANK SCHOOL

POLICY FOR ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION INCLUDING THE INTERNET

PURPOSE

The purpose of this policy is to establish the way ICT facilities and resources provided to members and Staff in order to perform their duties must be used. This policy has been developed to advise staff regarding if, when, and under what conditions they may use the Local Authority's communications and information systems for personal use.

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities; including teaching, research, administration and management. The school's Acceptable Use of Communications and Information Policy (including the Acceptable Internet Use Statement) has been drawn up in conjunction with Cheshire West and Chester's 'Acceptable Use Policy' in order to protect all parties – the pupils, the staff and the school.

This policy covers all forms of communication, information retrieval (from any source), media and equipment used regardless of origin, ownership or place of use, for example:

- internet and intranet (email, web access and video conferencing)
- telephones (hard wired and mobile)
- pagers
- fax equipment
- computers/iPads
- photocopying, printing and reproduction equipment
- recording / playback equipment
- Smart watches

This policy should be read in conjunction with **Appendix 4.10** of the Personnel Handbook.

This policy applies to all employees. A copy is available in the staffroom policy file and in class policy files. It is explained as part of the Induction Procedure.

USE OF FACILITIES

Staff must not carry out personal activities during work hours.

Office equipment and materials should not be used for private purposes or taken from work without prior permission from the School Business Manager, Deputy Head or Headteacher. Any information created or held on ICT systems will not be considered personal by default. It may, however, be deemed to be personal when reviewed by

the Information Assurance Team when authorised to identify if it is of a personal private nature. This includes email and internet communications.

Staff may use school telephones for private business, during break times, but should enter the length and destination of the call in the telephone book in the Administration Department. A charge will be made at the end of each term. Payment is not required when employees need to phone to notify someone they have been delayed at work or in other emergencies.
Staff may use the photocopier for reasonable amounts of private business provided they record the use in the phone book as above. A charge will be made at the end of the term.

The use of school mobile phones for personal business is not permitted. Personal mobile phones should not be used during teaching hours nor at break time/lunch time in the reception foyer or corridors.

Where an employee needs to discuss personal information with Occupational Health, Personnel or their Trade Union, they will be given permission and the privacy to do this.

You must keep your passwords confidential (don't share them with anyone else) and comply with password security arrangements. The main requirements being:

- At least eight characters - Contain characters from three of the four categories: uppercase; lowercase; 0 through to 9; or special characters (*&^%$£"! etc.)
- Are more complex than a single dictionary word (such passwords are easier for hackers to crack).
- Do not contain two of the same characters consecutively.
- Never reveal or share your passwords to anyone and never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Council systems.
- Do not use the same password for systems inside and outside of work

ACCEPTABLE INTERNET USE STATEMENT

- All Internet activity should be appropriate to staff professional activity or the students' education;
- Pupils will not be allowed access to the internet without supervision;
- Users are responsible for all email sent and for contacts made that may result in email being received. Staff are advised to consider marking any communication clearly as 'personal private' in the subject header. This helps ensure that personal information is treated accordingly;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;

- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- The school's email and internet facilities may only be used for personal use in very exceptional circumstances and then only after receiving permission from a member of the Senior Leadership Team.
- When using ICT Systems you must make sure that you communicate in a way that supports the relevant school policies and procedures that are specific to your role as well as corporately adopted, including those on equalities. You should therefore make sure that you do not send/upload/post information on-line which:
  - damages the organisation's reputation or undermines public confidence in Cheshire West and Chester Council, its staff, councillors, role or services;
  - supports political activity (other than any required in your role);
  - includes any libellous, offensive or defamatory material about any individual, firm, body or organisation; or
  - could be deemed to harass, bully or stalk another person.

It is not acceptable to use the school's equipment and materials in any of the following contexts:

- Illegal activity;
- Activities for private gain;
- Personal shopping;
- Personal photographs;
- Excessive personal messages;
- Gambling;
- Political comment or any campaigning;
- Personal communications to the media;
- Use of words or visual images that are offensive, distasteful or sexually explicit;
- Insulting, offensive malicious or defamatory messages or behaviour;
- Harassment or bullying;
- Accessing sites which could be regarded as sexually explicit, pornographic or otherwise distasteful or offensive;
- Actions which could embarrass the school or bring it into disrepute;
- Staff must not visit sites, make, post, download, upload or distribute any materials, remarks, proposals or comments that contain or relate to promoting political extremism or radical/religious extremism.

USE OF SOCIAL MEDIA

When you are using social media you must behave in accordance with the details set out in the Social Media Policy. Acceptable use of social media includes:

- When using social media sites you must not publish or post any information that you have received or have access to as a result of your employment unless you have been given permission to do so as this is confidential to your work
- You must not use social media sites in any way that may undermine public confidence in the school or your role within the school, bring the organisation into disrepute, or would be discriminatory or defamatory e.g. publish or post any

information including comments, jokes, illegal or prohibited images or other materials which would put the school at risk of legal action.

- You should avoid informal personal contact with service users you work with directly or indirectly, or their carers, through social media sites (e.g. do not add them as a 'friend', 'follow' them or link with them), or using your own personal electronic equipment (e.g. email, text, calls).
- You must not use social media to harass, bully, stalk or behave in any other way that could damage your working relationships with your colleagues, members of the public or elected members.
- Be aware that personal use of social media, while not acting on behalf of Rosebank, could potentially damage the organisation if an individual is recognised as being an employee. Any communications that employees make in a personal capacity through social media must therefore adhere to the principles as set out in the Social Media Guidelines.
- Whilst in work, employees are not allowed to access social media on school equipment with the exception of specific members of staff who are required to update the school's Facebook Page.

INADVERTENT ACCESS TO INAPPROPRIATE SITES AND INAPPROPRIATE EMAILS

If an employee inadvertently accesses an inappropriate website, they should leave it immediately and notify their manager of the incident, giving the date and time, web address (or general description) of site and the action taken. This will help safeguard their position in circumstances where disciplinary action would otherwise result.

Employees may find themselves receiving emails which contravene this policy. In the case of comparatively innocuous material (e.g. 'clean jokes'), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the school's policy. If there is repetition, the employee should retain the messages and notify their manager. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the manager notified immediately. Employees should notify the sender that they do not wish to receive further such material and keep a record of doing so.

CONSEQUENCES OF BREACH

Breaches of this policy may result in the application of the Disciplinary Procedure and may, if deemed sufficiently serious, be treated as gross misconduct. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

All staff should sign a copy of this Acceptable Internet Use Statement.

Name: Class:

Signed: Date:

Access Granted: Date:

Reference - Appendix 4.10
'Communications and Information Acceptable Use Policy' - CWAC

INTERNET ACCESS POLICY

Rosebank School believes that the educational benefits of internet access far outweigh the possible risks and that good planning and management will ensure appropriate and effective use by pupils and staff. The internet can be used by pupils of all ages and staff including admin and management.

WHY IS INTERNET ACCESS IMPORTANT?

- The purpose of the internet in school is to increase the opportunities for pupils to access a wider range of resources in support of the curriculum.

- It supports the professional work of staff and enhances the school management information and business administration systems.

- Access to the internet is a necessary tool for staff and pupils.

WHAT ARE THE BENEFITS TO THE SCHOOL?

The Government set targets for ICT use in all schools through the National Grid for Learning Initiative. A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the internet in education.

At Rosebank School this will include:

- Access to world-wide educational resources e.g. museums and art galleries;
- Enhancement of schemes of work in particular those relating to access of the internet for various activities;
- Inclusion in government initiatives such as NGfL, Curriculum Online, the Virtual Teacher Centre and specialist websites;
- Information and cultural exchanges between students world-wide;
- News and current events;
- Discussion with experts in many fields for pupils and staff;
- Staff professional development – access to educational materials and good curriculum practice;
- Communication with the advisory and support services, professional associations and colleagues;
- Exchange of curriculum and administration data with the LA and DfES.

We will encourage pupils to make effective use of the rich information resources available on the internet both for study and, where schemes of work dictate, recreation. We will encourage the pupils to develop the appropriate skills and understanding that will enable them to use these resources well and safely, as well as

the ability to analyse and evaluate the resources they find. These skills will be fundamental in the society our pupils will be entering. Pupils will be encouraged to make use of both the World Wide Web and email. Pupils will take part in e-safety assemblies, and complete e-safety work throughout the year. Children will have access to Chromebooks to work from home if they struggle to access the internet.

This information to be an addendum to the following policies:

- **Safeguarding Policy**
- **Acceptable Use of Communication and Information, including the Internet**
- **Guidance for Safer Working Practice for Adults who Work with Children and Young People in Educational Settings**

It is also to be included in the Staff Induction Pack.

SAFEGUARDING

Ensuring the safe and appropriate use of mobile phones

Rosebank recognise that staff may need to have access to their mobile phones during the working day. However they must be kept locked away during the day and must not be used in the classrooms or whilst staff are supervising children.
Staff must ensure that any phones brought onto school premises do not have any inappropriate or illegal content on them.
Phone calls must be limited to break and lunchtimes.
If staff feel they need to keep their phones with them for any reason during the day or make calls outside of these times, permission must be obtained from the SLT.
Mobile phone technology may not be used to take photographs of the children; there are digital cameras available to all classes and only these should be used to record visual information within the consent criteria guidelines of the school and local authority.
Photographs of children are not to be stored on laptops. Photographs may be stored only on school cameras, staff members' encrypted memory sticks and on the designated photograph memory sticks which are stored in a locked cupboard in the School Business Manager's office.
Only school printers are to be used for printing photographs of the children.
Members of staff may only contact parents and carers from a school landline or school approved mobile phone. When children are out of school on an educational visit or on a residential trip, any contact with parents must be made on an approved school mobile phone, except in emergencies and then only by approved telephones.
Staff, governors, volunteers and visitors must not comment or discuss any pupil or school related activities or upload pupil or school related photographs to social media sites.
Pupils should not bring mobile phones into school. If a child brings a phone into school, it will be kept in the school office until home time.

Use of mobile phones for Volunteers and Visitors

Volunteers and visitors to Rosebank will be advised on their initial visit, that they are not allowed to use their mobile phones on the school premises. If they wish to make or take an emergency call they must do so using the landline in the school offices or staffroom.
Volunteers, visitors, workmen and contractors are not permitted to take photographs or recordings of children without permission from the SLT and parents.



ROSEBANK SCHOOL
LAPTOP / iPAD LOAN FORM

Name
Equipment being signed for
Make Model Serial number

Conditions of loan

1. The laptop/iPad remains the property of Rosebank School.
2. The laptop is allocated to a named member of staff/governor and is their responsibility.
3. Only Rosebank School staff/governors should use the laptop/iPad.
4. On the staff member/governor leaving Rosebank School, the laptop should be returned to school. Staff on extended leave should return their laptops to school (unless otherwise agreed by the Headteacher).
5. The laptop must not be taken abroad.
6. Any software loaded must not affect the integrity of the school network.
7. If any removable devices/media are used they must be checked to ensure they are uncorrupted and virus free.
8. It is the responsibility of the staff member/governor to ensure virus protection is up to date.
9. Staff/governors should not attempt to significantly alter the computer settings other than to personalise their desktop area.
10. Students must never use staff/governor laptops.
11. If any fault occurs it should be reported to the ICT Technician.
12. A carrying case should be used when the equipment is being transported.
13. Laptops should be covered by normal household insurance. It is the responsibility of the staff member/governor to check this. If not the equipment should be kept in school in a locked place overnight.

I agree to abide by the above conditions for this loan.

Signature …….. Date …….