Be your best self

EXHALL GRANGE
SPECIALIST SCHOOL

Staff Acceptable Use Policy

Responsible Staff	GG
Governors Committee Responsible	Full Governing Board or Headteacher
Date Approved	October 2023
Review Date	Annually

1. INTRODUCTION

The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the ICT Network Manager in the first instance.

All members of staff have a responsibility to use the school's computer system and equipment in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system or equipment may result in disciplinary action (including possible termination of contract), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school and the requirements to protect sensitive data.

1.1 The internet and e-mail play an essential role in the conduct of our business in school.
The systems within school are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been a substantial investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.

1.2 How we communicate with people not only reflects on us as individuals but on the school. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of e-mail and the internet.

1.3 We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

1.4 For your safety, we are able to monitor all web pages visited, email sent and received. This helps us monitor inappropriate use, such as bullying.

1.5 This policy applies to you as an employee whatever your position, whether you are a Headteacher, Teacher, support staff, permanent, temporary or otherwise. Any inappropriate use of the school's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.

1.6 It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Headteacher or your line manager. Once you have read and understood this policy thoroughly, you should confirm your acceptance on the Every Compliance portal.

2. GENERAL PRINCIPLES AND LEGAL ISSUES

2.1 All information relating to our pupils, parents/carers and staff is confidential. You must treat all school information with the utmost care whether held on paper or electronically.

2.2 Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.

2.3 We trust you to use the internet sensibly. Please be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school.

2.4 The main advantage of the internet and e-mail is that they provide routes to access and disseminate information. However the same principles apply to information exchanged electronically in this way as apply to any other means of communication. For example, sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

2.5 Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher.

2.6 As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the school where it is necessary for your duties. The processing of personal data is governed by General Data Protection Regulations (GDPR) 2018. You should receive annual training to ensure compliance with GDPR and ensure all data is held securely and only hold data that is absolutely necessary to perform your professional duties. It is the responsibility of the school and the Local Authority as the data protection officer, to ensure that compliance is achieved.

2.7 All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

3. MONITORING COMMUNICATIONS

3.1 This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

3.1.1 To establish the existence of facts

3.1.2 To ascertain compliance with applicable regulatory or self-regulatory practices or procedures.

3.1.3 To ascertain or demonstrate effective system operation technically and by users.

3.1.4 For national security/crime prevention or detection.

3.1.5 For confidential counselling/support services.

3.1.6 For Investigating or detecting unauthorized use of the system

3.1.7 For monitoring communications for the purpose of determining whether they are communications relevant to the business.

3.2 Warwickshire LA has an obligation to monitor the use of the internet and e-mail services provided as part of the Warwickshire Broadband service to schools, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. Warwickshire LA and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications

3.3 If the email is personal, it is good practice to use the word `personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

3.4 Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the school's business purposes which include the following:

3.4.1 Providing evidence of business transactions;

3.4.2 Making sure the school's business procedures are adhered to;

3.4.3 Training and monitoring standards of service;

3.4.4 Preventing or detecting unauthorised use of the communications systems or criminal activities.

3.4.5 Maintaining the effective operation of communication systems.

3.5 Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.

3.6 You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).

3.7 The school may also use measures to audit use of computer systems for performance and diagnostic purposes.

Use of the school computer system indicates your consent to the above described monitoring taking place

4. USE OF INTERNET AND INTRANET

4.1 When entering an internet site, always read and comply with the terms and conditions governing its use.

4.2 Do not download any images, text or material which is copyright protected without the appropriate authorisation.

4.3 Do not download any images, text or material which is inappropriate or likely to cause offence.

4.4 If you want to download any software or Apps, first seek permission from the Headteacher and/or member of staff responsible. They should check that the source is safe and appropriately licensed and conforms with GDPR.

4.5 If you are involved in creating, amending or deleting our web pages or content on our web sites, such actions should be consistent with your responsibilities and be in the best interests of the school.

4.6 You are expressly prohibited from:

- 4.6.1 Introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- 4.6.2 Seeking to gain access to restricted areas of the network;
- 4.6.3 Knowingly seeking to access data which you are not authorised to view;
- 4.6.4 introducing any form of computer viruses;
- 4.6.5 Carrying out other hacking activities.
- 4.7 For your information, the following activities are criminal offences under the Computer Misuse Act 1990:
- 4.7.1 Unauthorized access to computer material i.e. hacking;
- 4.7.2 Unauthorized modification of computer material;
- 4.7.3 Unauthorized access with intent to commit/facilitate the commission of further offences.

4.8 Social Networking

Staff should take care when using social networking websites such as Facebook or MySpace, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You should not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your ‘friends list’.
- You must ensure that personal information is not accessible via a ‘Public’ setting, but ensure it is set to a ‘Friends only’ level of visibility.
- You should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

4.9 Online Forums

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school’s reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

5. USE OF ELECTRONIC MAIL

5.1 You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure. E-mail within the domain @exhallgrange.co.uk is the only secure e-mail authorised by the county, all other e-mail address would require information to be encrypted and the password sent in a separate communication.

5.2 Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is `Confidential’ in the subject line

5.3 Copies of emails with any attachments sent to or received from parents/carers should be saved in a suitable secure directory.

5.4 Do not impersonate any other person when using e-mail or amend any messages received.

5.5 It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

5.6 E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school or about its students.

5.7 Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school e-mail account will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet or access to your own private e-mail through the schools network or using a school terminal.

See Appendix 1 for guidance on sending emails.

6. DATA PROTECTION

6.1 Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the school's premises or working remotely you must:

6.1.1 Keep the data private and confidential and you must not disclose information to any other person unless authorized to do so. If in doubt ask your Headteacher or line manager;

6.1.2 Familiarize yourself with the provisions of the General Data Protection Regulations 2018 and comply with its provisions;

6.1.3 Familiarize yourself with all appropriate school policies and procedures;

6.1.4 Do not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the school holds on them.

6.2 The school maintains reports for any breach of the GDPR and this can be viewed as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.

6.21 All staff must report any possible breach of data immediately to the designated Data Champions or Headteacher, a log of the incident will be taken and when necessary forwarded to the Data Protection Officer and/or **Information Commissioner's Office**.

6.3 If you make or encourage another person to make an unauthorized disclosure knowingly or recklessly you may be held criminally liable.

6.4 You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone, including IT support staff, friends, family or colleagues. If you do so, you must request to change your password immediately.

6.5 You must not allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.

6.6 When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence using the Ctrl Alt and Delete keys and choosing the appropriate option.

6.7 You must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and supplied or approved for such use by the school.

6.8 You must not transmit any sensitive or personal information about staff or students via email without the data being encrypted with a password and this sent via a separate communication, you should ask the ICT Network Manager which method is approved for the school.

6.9 If you use a personal electronic device at home for work purposes, you must ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft, you must not use auto store/remember password facilities.

6.10 You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.

6.11 Equipment taken offsite is not routinely insured by the school. If you take any school computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft, in addition you are responsible for its security at all times.

7. USE OF OWN EQUIPMENT

7.1 Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school’s normal rules on electrical safety testing.

7.2 You must not connect personal computer equipment to school computer equipment without prior approval from IT Network staff, with the exception of storage devices such as USB memory sticks.

7.3 If you keep files on a personal storage device (such as a USB memory stick), you must ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the school computer system.

8. SUPERVISION OF PUPIL USE

8.1 Pupils must be supervised at all times when using school computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.

8.2 Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.

8.3 Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

9. REPORTING PROBLEMS WITH THE COMPUTER SYSTEM

It is the role of the ICT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

9.1 You should report any problems that need attention to the ICT Network Manager as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem must be reported via the online support request system.

9.2 If you suspect your computer has been affected by a virus or other malware, you must report this to the ICT Network Manager immediately.

9.3 If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

10. REPORTING BREACHES OF THIS POLICY

10.1 All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of SLT, or the ICT Network Manager, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.;
- Any breaches, or attempted breaches, of computer security; or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

10.2 Staff must inform the ICT Network Manager in writing immediately of abuse of any ICT system(s) - software and hardware - providing the location and names where possible.

10.3 Reports should be made either via email or the online support request system. All reports will be treated confidentially.

Once you have read this policy, you MUST confirm through the documents section of the Every Compliance portal that you have read and understood it.

APPENDIX 1

Guidance for sending Emails

To: Ensure this is sent to who you want a reply from or the information to go to.
If you are asking a questions, putting in more than 1 or 2 people causes confusion.
It should only be To: the person you need to action/respond.

CC: Is for informing a person/people about something but not for expecting a response.

Subject: Ensure this is completed.

Start of Email: Dear ….,

Close of Email: Kind regards,
First name
Full Name
Role
Exhall Grange Specialist School
Easter Way
Ash Green
Coventry
CV7 9JG
Telephone : 024 7636 4200

- When replying to an email, ensure you 'reply all' if there is more than one person in the 'To:' or 'CC:'

- Staff emails to each other and externally, should be limited to 7 am and 7 pm.

- Staff are expected to/can respond to parents/carers between 7 am and 5 pm.

- An automatic response of "your email will be responded to within 48 hours" must be set up outside these times.

- A 'holding' email can be sent if deemed appropriate, 'I acknowledge receipt of your email and will respond within 24 hours or 48 hours'.

- When sending emails, ask the question, would a conversation/meeting in person be more appropriate/productive/efficient use of time.