Birmingham Federation
Maintained Nursery Schools

IT USER POLICY

Cluster:
Gracelands Nursery School
Jakeman Nursery School

Local Committee Approved: 22 October 2024

Full Governing Body Approved: 09 December 2024

Date Policy Adopted: 22 October 2024

Date for next renewal: Autumn Term 2026

Chair of Governors: Sean Delaney

Executive Head Teacher: Samantha Richards

Contents

1. Rationale

1.1 From time to time, amendments to the Acts of Parliament and the introduction of new Acts of Parliament require our schools to update its I.T. Policy and regulations. All staff within our schools are required to accept the agreed policy and regulations electronically during the computer network logon process, or when they initially open a new account, before access to systems is authorised.

1.2 From time to time, amendments to the Acts of Parliament and the introduction of new Acts of Parliament require our schools to update its I.T. Policy and regulations. All staff within our schools are required to accept the agreed policy and regulations electronically during the computer network logon process, or when they initially open a new account, before access to systems is authorised.

1.3 Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Executive Head Teacher or Head of School for approval.

1.4 This Policy applies to staff and is an independent document, but for the purposes of this policy are appended to it. Staff are also advised to abide by the school's Electronic Mail Etiquette when using email. This is attached as Appendix 2. It is advisory and does not have the force of the regulations; however severe or excessive breaches may result in disciplinary action, and the guidelines would be referred to in the event of any complaint. Staff should be aware that the use of computing facilities is governed by legislation including:

The Data Protection Acts (1984 and 1998);

The Copyright, Designs and Patents Act (1988);

The Computer Misuse Act (1990);

The Criminal Justice and Public Order Act (1994); Amending the Obscene Publications Act (1956);

The Protection of Children Act (1978);

The Telecommunications Act (1984);

The Human Rights Act (1998);

The Regulation of Investigatory Powers Act, 2000.

Any breach of these Acts will result in action being taken under the terms of the school's disciplinary policy and may be further escalated to law enforcement officers.

1.5 Staff with proper authorisation may use the internet and email facilities belonging to the school, providing that they observe the regulations, U.K. legislation and avoid the disruption of services for other users.

2. Policy

2.1 It is the policy of our schools to provide access to the internet and an email service for the use of staff and children, to facilitate reliable communications and to provide direct access to readily available sources of information for teaching, research, learning and school business needs.

2.2 In particular, the use of the Internet as a valuable tool and source of information is acknowledged; and the principles of academic freedom in access to and downloading of source data and contributing and exchanging information and opinion are incorporated into this policy.

2.3 Notwithstanding the above and although internet web site usage and email messages are not regularly monitored, our schools reserve the right to intercept communications for inspection (in line with the Regulation of Investigatory Powers Act, The Data Protection Act and the Freedom of Information Act) should an incident occur where inappropriate use of the facilities is suspected. Any violation of the provisions (for example, downloading pornographic material, sending offensive messages, harassment, discrimination, spamming or hacking) may result in action up to and including dismissal under the Disciplinary Policy of our schools. In the event that IT User Policy legislative requirements (for example, any of the above Acts of Parliament) are breached, then the perpetrator(s) will also be subject to legal action.

2.4 It is important that all users understand and appreciate the values and dangers of using the Internet and email systems and follow the principles of the policy and the terms of the associated regulations and email guidelines in order to safeguard their interests and those of our schools. It should be noted that messages and data transmitted internally and to external

sources are the property of our schools and that all users have a responsibility to safeguard electronically accessed information against loss, disclosure or misuse.

2.5 Breaches of this Policy, the Regulations and in cases where there are irregularities, the perpetrators will be subject to school disciplinary processes and the law.

3. Internet Usage

3.1 Internet software may only be installed by or with the agreement of the Executive Head Teacher. No unapproved or downloaded software may be used unless the integrity, continuity and full support of the product can be guaranteed. Software patches or updates may only be downloaded from officially supported vendors, subject to the consent of the Executive Head Teacher and ensuring strict adherence to the vendor's security and usage guidelines.

3.2 Our schools provide access to the Internet and its resources for the purposes of teaching, research and other school business. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out in the policy and regulations. Personal use must not interfere with the operation of school services, involve cost implications for the school/s or take precedence over the user's work accountabilities.

3.3 Our schools reserve the right to block access to any Internet resource. Academic access to blocked sites may be arranged on application via the Executive Head Teacher.

3.4 As indicated under section 2.3, staff, must not access, retrieve, print or distribute text or graphical information that is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory, pornographic or otherwise obscene; defamatory or libellous or any other material which contains illegal content prohibited by law or regulation.

3.5 Similarly, to protect school systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted. Where such use is suggested for training or development purposes, it must have the specific agreement of the Head Teacher.

3.6 Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the school network or the internet or bypass security features.

4. Email Usage

4.1 Email users should be aware that the boundaries between internal and external mail are now very blurred and it should not be assumed that email will remain within the school network.

4.2 Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or libellous or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation or which brings our school/s into disrepute or which contravenes our policies. Information is understood to include text, images, sound and video; transmission is understood to include printing information and sending information via email. In particular, with respect to defamatory or libellous statements about another internal or external party, it should be noted that emails are discoverable documents in legal actions and may be used in evidence under the Regulation of Investigatory Powers Act (2000).

4.3 All material contained on the email system belongs to our schools and staff should not consider messages produced / received by them on school equipment/software (owned or licensed) to be secure. The confidentiality of email cannot be assured and staff should be aware of the possibilities of intended or accidental onward transmission to others beyond the original addressee(s). Furthermore, it is possible to retrieve deleted emails from backed up files intended to assure system integrity and reliability.

4.4 Security regarding access to the email system is of paramount importance as indicated in the regulations. User identities and personal passwords must not be shared with others and staff should be wary of providing their email addresses to external parties, especially mailing lists.

4.5 Staff transferring or receiving files or attachments from external sources should note that our school systems automatically check downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the Executive Head Teacher immediately for inspection and action.

4.6 School email users are required to use this communication tool in a responsible fashion and to observe the related Regulations. Our schools provide the email system for the purposes of conducting school business and it may not be used for personal gain or business activities unrelated to school operations. Staff must not use the system to promote an external cause or fundraising campaign without advance line management permission.

4.7 Reasonable personal use of the email system is permitted, subject to the approval of the Executive Head Teacher and the constraints and conditions set out in this Policy and the Regulations. The Head Teacher may define the level of use, as appropriate, in their areas.

Personal use must not interfere with the operation of school services, involve cost implications for the school/s or take precedence over the user's job accountabilities.

4.8 Authorisation to use the school's computer devices at home or school software on home PCs will be withdrawn on the termination of the employee's contract of employment and computer records of emails sent and received will be destroyed after a suitable period of time by the IT Services Department.

4.9 Where it is considered that there has been a breach in the use of the email system, any intercepted emails will be referred to the School Directorate for examination of the contents.

5. Responsibilities

5.1 Our schools are responsible for the administration of this policy and the regulations for the use of school computer systems, networks and facilities. Overall accountability for data protection within our schools' rests with the registrar and clerk to the Governors, although operational responsibility for staff data is held by the school Office Managers. However, all members of the Senior Leadership Team are responsible for the conduct and performance of their staff, their usage of school facilities and equipment and their adherence to the contents of this policy and the regulations, including General Data Protection Regulation (GDPR) 2017.

5.2 Every school computer device user agrees to abide by the terms and conditions set out in this policy and the regulations. Every user must accept responsibility for the protection of electronically accessed information against loss, disclosure or misuse.

5.3 All users must be aware of their responsibilities and obligations to others under the terms of the data protection legislation. Particular care must be exercised in respect of data held about other people both inside and outside the school for operational, research or any personal purposes. Both the IT Policy and the associated regulations have the same status as a contract of employment.

APPENDIX 1 REGULATIONS FOR THE USE OF SCHOOL COMPUTER SYSTEMS, NETWORKS AND FACILITIES

These regulations should be read in conjunction with our Acceptable Internet Usage statement and agreement/ eSafety Policy. Suspected misuse or abuse of school systems must be reported to the Executive Head Teacher.

Introduction

• In general, members of the school workforce may use those computing facilities that they are authorised to access providing that the use is related to their job (for staff) and the curriculum (for children). Modest use for private non-academic purposes is usually acceptable, however users must recognise that such use must not adversely affect the operation of the school/s. Staff should refer to the IT User Policy on this and other related matters. There are some activities that are expressly forbidden, because:

- They are illegal;
- They may disrupt services for others, and / or incur unnecessary cost for the school/s.

• The purpose of these regulations is therefore to protect the interests of users and to ensure that our schools remain within the law. We reserve the right to monitor network traffic activity and material held on the systems (within the legal constraints of the Data Protection Act and The Regulation of Investigatory Powers Act), in order to ensure that users are complying with these regulations.

• User material, or access to user material, may be removed if there are grounds for believing that it is in breach of the law or of these regulations. In summary the regulations are:

- Users must comply with current UK legislation relating to the use of data networks, computers and computer held information;
- Users must not attempt to gain access to systems or information for which they are not authorised;
- If use is made of links to external networks and facilities, the regulations governing the use of these facilities must be adhered to;
- Users must follow the school guidelines for maintaining security of systems;
- Users must follow our school policies covering electronic communication;
- Users must comply with practices to protect against computer viruses and other malicious acts;
- Unauthorised copying and/or installation of software is strictly forbidden and will be reported to external authorities.

Penalties

• Withdrawal of Facilities Failure to adhere to these regulations may lead to withdrawal or restriction of access to school computing facilities, following discussion with the Head of School / Head Teacher.

Disciplinary Procedures

• Any breach of regulations by staff or students will be reported and deal with under the school's disciplinary procedures and if any action contravenes the Acts of Parliament listed above, law enforcement officers will be involved.

• Actions in breach of the law all illegal action will be immediately reported to the police.

• Computer related UK Legislation The major UK legislation applicable to computer and network use is referred to below. This document can only offer very general guidelines on the legislation. For further information please contact the Executive Head Teacher who will be able to suggest sources of more detailed information.

• The Computer Misuse Act (1990). It is an offence to access, or try to access, any computer system or material for which authorisation has not been given. Any attempt to bypass security controls on a computing system is also an offence, as is facilitating unauthorised access, by, for example, the disclosure of a user id or password. The majority of our school computers are networked, and it may be possible to connect to computers both within and external to our schools, some of which may offer public services. However, being able to connect to a computer system does not necessarily mean that access to it is authorised.

• The Copyright, Design and Patents Act (1988) Almost all computer software in use within our schools is protected under this Act, which gives the owners of the copyright the exclusive right to copy a protected work. It is therefore illegal to copy any software without the copyright owner's permission. Software may only be used for the purposes defined in the licensing agreement, and on the computer systems to which that agreement applies. Terms and conditions of license agreements vary considerably from product to product. Further advice may be obtained from Link 2 ICT for any particular case. Users must also ensure they have the permission of the copyright holder to publish material on web pages under their control.

• The Data Protection Act relates to the automatic processing of personal data that is information relating to a living person, and is applicable to computerised and also some manual systems. The Act gives individuals certain legal rights regarding information held about them by others, and sets requirements for organisations to meet before personal data can legally be processed. Staff who process personal data must ensure that they comply with the Act, and if in doubt must refer to their line manager. It should be noted that the automatic processing of personal data includes data that may be contained in email messages.

• The Criminal Justice and Public Order Act (1994) This Act extends the scope of the Obscene Publications Act 1959 to make the storage and electronic transmission of obscene material arrestable offences. It is expressly forbidden to use school facilities for the downloading and / or

storage of pornography. Transgressors will be subject to disciplinary procedures and may be reported to the police.

• The Protection of Children Act (1978) Relating to images of children transmitted, sourced or created using computers The Regulation of Investigatory Powers Act (2000) This Act repeals prior legislation in the area of interception of communications Act (1985) and implements article (5) of the EU Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the communications sector.

Authorised Use

• All staff within our schools will be registered to use the computer facilities for the purposes of their academic studies or school employment. Upon registration or commencement of employment a computer account will be created and the new user issued with a unique username. All staff network users will be required to sign acceptance of these regulations in the Acceptable Internet Use Statement. On occasions some visitors and conference delegates may apply through the designated co-ordinator for registration and access to the computer network, whereby a small administrative fee is payable. Our schools reserve the right to refuse access.

• Individually allocated user names are for the exclusive use of the person to whom they have been issued. This person is responsible and accountable for all activities carried out under their username. Attempts to use a username not authorised to the user is prohibited. In particular, passwords must not be disclosed to any other person, and good practice in the selection and use of passwords must be adhered to. Further details regarding such good practice may be obtained from Link 2 ICT, but in general:

• A password should be chosen carefully. It should not be a name or proper word, and should preferably include some digits;

• Passwords must be changed regularly (every three months is reasonable for most users);

• All users must identify themselves correctly at all times, and must not attempt to withhold their identity or masquerade as another.

Virus Protection

A virus is a program written to cause intentional damage to computer systems or networks, generally replicating itself from computer to computer across a network (downloaded from the internet or as an attachment to an email message) or from the distribution of an "infected" external media device such as CD, DVD or USB flash memory. The degree of damage caused varies, but many viruses destroy data and can significantly impair system operation. Virus scanning software has been installed on all networked PC systems in our schools, and may be available under the terms of the software license for installation on home computers. However, all users must take the necessary steps to protect school systems from viruses by adhering to the following rules:

- Any software programs must not be installed or executed without the prior approval of IT Services, and in particular:
- Computer Games;
- Public domain software, shareware or peer to peer software;
- Any unauthorised program attached to an email message;
- Any programs obtained from the Internet. The following categories of computer media must always be scanned for viruses:
- Any originating from outside our school/s network/s;
- Any used on a home computer;
- Removable storage devices such as CD's DVD's or USB flash memory;
- Computer magazine cover disks;
- Free mailings.

Unacceptable Use of School IT facilities

In addition to the above, the following are specifically defined as unacceptable usage of our school computers and networks. This list is not necessarily exhaustive. School systems and networks must not be used for:

- Copyright infringement or plagiarism;
- The sending of messages which are racially, sexually or personally abusive;
- The corruption or destruction of other user's data;
- The initiation or spread of electronic chain mail or SPAM;
- Any activity which is wasteful of resources such as playing of computer games;
- Defamation or libellous attacks on persons;
- Any activity that may reflect adversely upon our school/s. Behaviour in the Nursery and Offices
- It is suggested that no food or drink should be consumed in offices and strictly no food or drink in the Nursery, as those responsible for any spillage resulting in damage to equipment will be held accountable for the cost of repairs;
- Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities.
- No equipment should be moved from its designated place or be tampered with in any way. This includes changing workstation characteristics;
- Users should not act in a way so as to deliberately, or recklessly, overload access links or switching equipment;
- Printer stationery should be used for the purpose for which it is supplied. The theft of printer paper will be dealt with seriously.

Disclaimers

Our schools accept no responsibility for the malfunctioning of any equipment or software, nor failure in security or integrity of any stored program, data, email content or Internet download. No

claim shall be made against our schools, their employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the Institution, its employees or agents. Our schools will not be liable for the content of email messages or any attachments therein and the text of said emails does not reflect the views of our schools, the Board of Governors or staff.

APPENDIX 2 Email Etiquette

Introduction

• Electronic mail is one of the primary means of communication but because it is perceived as quick and easy conventions as to how it is used are not well developed. Although email is more flexible and in some ways easier to use than a traditional format, it has its own limitations and can still be used in a Court of Law as evidence of a wrongdoing.

• This paper sets down some points of good practice for both senders and receivers of email to help us make more effective use of this medium. 2. Some characteristics of email in considering the use of email, it is worth noting some of its characteristics, which should influence how we use it.

• Email cannot be regarded as private or secure. Avoid sending confidential information via email unless an encryption tool is available;

• Messages cannot be totally erased; even when deleted they can be retrieved from backups and usually traced back to their origin;

• Messages can be stored; unlike telephone conversations they are not ephemeral;

• Messages can be printed, so cannot be regarded as purely electronic;

• Messages can be readily sent to a large number of recipients and forwarded many times;

• Forwarded messages can be invisibly edited (unlike a memo, which is fairly obvious if it's been altered).

• Depending on the way in which the message was sent, recipients who are on a distribution list may be unaware that they are not the only ones to receive the message. They also may not know who the other recipients are.

Sending Email

• Is email really the most appropriate medium? If you are composing a message that is long or requires some care in its construction, language and presentation, ask yourself whether a letter or memo might be more appropriate;

• Messages should be short and to the point. A message that makes its point and fits on one screen does its job best;

• Clearly identify the topic in the subject field;

• A message should be about a single topic. If you want to raise a second topic, send another message to avoid having content unrelated to the message heading;

• If you need to cover several related topics, try to make the subject label broad enough to cover the whole. Multiple topics are confusing and frustrating for someone trying to follow a thread through email correspondence;

• You can never be sure what system your recipients will use to view your message. Although email systems like Outlook encourage you to format your messages, this formatting may not survive to your recipient. For this reason it is a good idea to treat all messages as plain text (and avoid using £ signs, use GBP instead);

• Use appropriate spelling, grammar and punctuation. Always proof read and use the spell checker if necessary. Messages are frequently printed and errors that may be overlooked or excused when read on screen are likely to be judged more harshly when seen on paper;

• Choose words carefully, sometimes hastily produced messages can be misinterpreted. Avoid slang;

• Don't include anything that you would have reservations about appearing in print above your signature;

• Be careful of your 'tone of voice'. Because your facial expressions and verbal tone are missing from electronic correspondence, your text is open to misinterpretation;

• Avoid sarcasm or other forms of dry humour to minimise the risk of misinterpretation;

• Do not use all capitals, as it may be interpreted as SHOUTING;

• You should make it clear if you do not wish your message to be forwarded by its first recipients;

• Think carefully about sending confidential information about yourself or others. If your message refers to a colleague or their work make sure you include that colleague in the circulation of the message.

Replying to email

• If possible reply within 24 hours. If you cannot answer a message within this time, send a message saying when you will be able to respond;

• Consider using 'Sabbatical' when on leave or out of the office for any period of time making sure you give a contact name for urgent messages. However, remember that if you are on a mailing list it can be irritating to receive "Out of Office" messages from unknown individuals;

• Change the subject line if the topic changes in your reply;

• Use a signature that gives contact information, i.e., extension number and department;

• Do not include the original message automatically. Consider whether it is necessary e.g., where the recipients of your reply include people who did not receive the original;

• Without sacrificing brevity unduly, try to make your reply intelligible on its own, without referencing back to the original message;

• When responding to a message sent to several colleagues, check whether anyone else has already responded;

• When replying to a message that has been sent to a list of recipients, only reply to the whole list if your answer is of interest to them all If you are taking up specific points with the sender of the original message, send your response only to that person;

• Watch ccs when replying to make sure you reach your intended audience and to reduce the volume of unnecessary material sent to others.

Forwarding email

• Take care in forwarding a message: would the original sender wish you to do so? You may need to seek their permission first;

• It may be a good idea to remove a lengthy distribution list from the head of a message before forwarding it. If you do this (or make other changes), it would be appropriate to write a note, indicating what you have done;

• If, instead of forwarding a message, you extract a chunk from it and send that as a new message, or as part of a new message, make sure your recipient knows you have edited the message;

• Be considerate to recipients of forwarded email by reducing the amount of unnecessary material included in the message.

Email addresses

• Where there is more than one user with similar names, check that you have chosen the right one.

• Users' internal email addresses do change from time to time so again check that you have chosen the right one and also keep any personal distribution lists up to date.

Email attachments and Filing email

• Email can be an extremely convenient way to send files, however, these files may be large and take up capacity on mail servers and this can seriously impair the performance of the email system.

• Think carefully before sending any message with an attachment to a large distribution list. Place it instead in a shared area and email people with the filename and its location;

• The mail server supporting the email system is not intended for the long term storage of messages. When you receive an email message with an attachment, save the attachment to your area on the appropriate drive.

• Housekeeping of stored messages is your responsibility. From time to time you should go through your stored messages, deleting those that are no longer needed;

Unwanted email

• Email can be an extremely convenient way to send files, however, these files may be large and take up capacity on mail servers, this can because the Internet is largely unregulated and it is difficult to prevent unsolicited messages reaching you. You can limit who gets hold of your email address by being circumspect when visiting web sites and by thinking carefully before subscribing to any mail service. However, lists of email addresses are bought and sold in the same way as lists of postal addresses are (but with less scope for regulation).

• Do not reply to 'junk' email, this indicates to the sender that your email account is 'live';

• The best way to deal with 'junk' email is to delete it.

• Think before you send email is an effective way of communicating but it is easy to be overloaded with emails if it is not managed properly, in which case the benefits will be lost. Please be aware that email communications can be presented as evidence in court of law and are legally binding.

APPENDIX 3 PROCEDURE IN THE EVENT OF ANY IMPROPER USE OF EMAIL OR THE INTERNET

• Where it is considered that there has been a breach in the use of the school email/ internet system the following Disciplinary Procedures will be put into practice.

• The IT Coordinator will notify a member of the Senior Leadership Team that they consider that there has been a breach in the use of the school computer system.

• The Senior Leadership Team will consider the facts presented and if it is considered that there has been inappropriate use the IT Coordinator will be instructed to disable the user's access until further notice.

• The employee's line manager will be notified of the incident. • The employee will be notified by the Head of Personnel that their computer access has been denied pending an inquiry into the inappropriate use of the school's computer system and the employee will be asked to attend a disciplinary hearing in accordance with the school Disciplinary Procedure.

• The recommendation from the civil police is that all incidents are reported to them, however, the Senior Leadership Team will review carefully the extent of any inappropriate usage before deciding to report the incident to the police. Any incident involving child pornographic material will be referred immediately to the police.

• In those circumstances where a member of staff is alleged to be in breach of the Code of Practice, such allegations will be investigated by the registrar and clerk to the Governors, the Head of Personnel, the IT Coordinator and an invited representative from the recognised trade union or staff association. The results of the investigation will be reported to the Executive Head Teacher who will ultimately decide if the school's Disciplinary Procedure should be invoked. In the event of any disciplinary action being taken the accompanying person /representative for the employee must not be the same invited person who took part in the investigation.