Glade Primary School

Acceptable Use Policy

Growing, **L**earning & **A**chieving with **D**edication & **E**nthusiasm

January 2019

Contents

1 Introduction

This policy has been developed to clearly state the expectations of Glade Primary School in respect of all persons using equipment, facilities and information belonging to the school.

This policy covers the use of:

- Equipment (including but not limited to computers, laptops, tablets and smartphones
- Internet
- Email

Failure to adhere to the Acceptable Use Policy will result in appropriate disciplinary action in line with the School's Disciplinary procedures. The School requires users to accept that:

- This policy applies no matter your work location i.e. in the school, at home, remote or mobile working.
- You **are** aware that improper use of any school information can result in either you and/or the school incurring civil or criminal liability so the school reserves the right to report any illegal activities to the appropriate authorities.

2 General conduct

As a user of the school's information and information systems, you are expected to act in a professional and responsible manner and therefore you **must not**:

- Attempt to make changes to information or information systems where you have no explicit permission or authorisation, or where any change made could be construed as fraudulent or illegal. This includes installing or attempting to reconfigure any software, or delegating such a change to another user.

- Make statements on your own behalf or on behalf of the school, using any of the school's communication channels, which are or may be defamatory, bring the school into disrepute or imply that you are acting on behalf of the school when you have no authority to do so.

- Knowingly carry out any action that will degrade or deny access to information to other users

- Use school systems to breach, or attempt to breach, any legislation. These include Protection of the Children Act; the Obscene Publications Act; the General Data Protection Regulations (GDPR); Data Protection Act; Freedom of Information Act; Intellectual Property Legislation; Copyright Legislation; and the Computer Misuse Act.

- Place school information at risk by handling it in an insecure manner within and outside of school premises.

3 Confidentiality

In order to maintain confidentiality

- Do not forward to an external party any information that may compromise the Information Classification Policy, or the rights of a service user or third party in relation to their confidentiality

Where you have received an email in error, notify the sender that you have

received the message in error and then delete any copies of misdirected message If the email contains sensitive or personal information notify the ICT Manager, Kevin Crouch, that information has been disclosed in error.

- Information should only be shared where there is a business need to do so and this should be in accordance with the Data Processing Agreement with the third party

4 Access control

To ensure only authorised users can access the school information and systems:

- You **must not** use a colleague's user name and password (credentials) to gain access to any information or system.
- You **must not** attempt to access any information or system that you have not been given explicit permission to access.
- You **must not** share your credentials or use them to log another person into the network even if you are asked to by your line manager.
- You **must** notify the loss of your credentials or where a third party gains access to your password, by reporting this to Rachel Banks, School Business Manager.
- You **must** notify the ICT Manager, Kevin Crouch, to disable your account as soon as you become aware of any unauthorised access using your credentials.
- You **must** lock your computer screen when away from your (computer) using the keyboard locking mechanism to protect on-screen information.

5 Email Usage

Email is an effective business tool for communicating with colleagues, parents, suppliers etc. inside and outside the school.

Email is not a secure means of communication. It does not provide immediate or guaranteed delivery.

All emails sent or received using the school's systems are the property of the school.

All messages will be unpacked and scanned for viruses as they arrive or leave all school systems.

Users of school Email **shall**:

- Send all sensitive information using ***Egress***. This will also indicate to the recipient how you expect them to handle the information
- Send confidential or sensitive personal information to general email addresses (e.g. Hotmail, yahoo, gmail, msn) using encrypted email; except where documented consent is given by the data subject
- Ensure emails never contain children's full names either in the subject line or the main body of the text. Initials should be used wherever possible.
- Use "Private" calendar appointments where the subject of meeting indicates confidentiality is of concern.
- Treat email as permanent written records which may be read by persons other than the addressee and store these in appropriate network locations in a structured manner according to their retention schedule
- Review their Email mailbox regularly and delete unnecessary messages

- Treat unsolicited Emails from unknown sources with suspicion

Users of school Email **shall not**:

- Use language which includes swear words, or be offensive or abusive.
- Send school information to or from your own personal email address especially where this includes sensitive personal information of a pupil or staff member
- Download school information to non-school devices or personally controlled cloud storage.
- Set up automatic forwarding of email rules to external email accounts
- Transmit PIN (personal identify numbers) or PAN (personal account numbers) used in credit card transactions via email or any other messaging systems unless appropriately encrypted.
- Send outbound email from generic email accounts set up to receive incoming email only
- Forward "chain" or joke emails to others
- Use school email addresses and other official contact details for setting up personal social media accounts.
- Rename email attachments or password protect attachments to evade malicious software scanning.
- Seek to gain access to another user's mailbox without either their consent or the written approval of their line manager

Where you are replying to messages from internet email accounts, take care to remove personal data from the correspondence chain where appropriate. The onus is on Glade Primary School to protect data in transit.

6 General Usage Guidance

6.1 Desktop / Laptop computers

Desktop/Laptop computers **must not** be used to store any data, including protectively marked or personal, sensitive data files. Data stored on the device are not backed up, and are at risk of loss, theft, or damage by viruses or other malicious software such as spyware.

You **must not** store any non-work related (i.e. not for school business) files, personally owned software or pictures on school owned computers or shared folders.

You **must not** store any non-work related video clips, pictures, graphics such as JPEG files, music files such as MP3 files, games, screen savers or desktop wallpapers on the home drives (eg: 'My Documents' folder), laptops or any other storage media such as USB devices issued by the school. This includes any similar files that may be downloaded from the Internet or personally owned.

It is school policy to monitor electronic file storage usage, and to remove any software or files deemed inappropriate or pose a risk to the school's information systems, break copyright legislation, or are not for work purposes.

6.2 Removable Media

All removable media **must** be approved before use on the school's computer systems and network. If you require clarification then contact the school ICT Manager. This is to prevent data loss, and to stop the school's computer systems being infected with malware e.g. viruses and key loggers.

If you are in possession of unencrypted portable media holding personal data, please contact the ICT Manager to arrange its collection and disposal.

6.3 Personal Use

The school recognises that occasional personal use of the school's computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Must comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.

- Must not interfere in any way with your other duties or those of any other member of staff.

- Must not have any undue effect on the performance of the computer system; and

- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Staff may use the school Email system and internet access for personal use, provided such use does not breach the officer's code of conduct and/or the school's constitution. Permitted personal use **must not** impact on your day-to-day work.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

- In addition, your: Personally owned computer equipment **must not** be connected to the school's data network except where this has been expressly authorised.

The School will not be liable for damage to personal items that are connected to its equipment E.g mobile phones being charged through USB ports.

6.4 Software and Downloads

All users are prohibited from installing software onto the network from a CD-ROM, other device or by downloading from the Internet without permission from the ICT Manager. If users need a new program installing onto the computer, our ICT Service Desk will be asked to do this if possible.

Copyright and intellectual property rights must be respected when downloading from the internet.

6.5 Images/Videos

Parental consent is required for all children under the age of 16 to have photographs or videos published electronically or in a public area even if they are unidentifiable.

No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

6.6 Network Protocol

The network protocol is as follows:

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy them.
- Do not open other people's files without expressed permission.
- When working with personal data ensure that the data is secure.

6.7 Internet Usage

- Ensure all Internet access is carried out under your login account only;
- Ensure that Internet access is for the purpose of your contractual obligations and that you do not either misrepresent your level of authority in these regards.
- Pupils must be supervised at all times when using the internet.
- Activities should be planned so 'open searching is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.

- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines. However safe search is set on all computers in school as a default on search engines.

- The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter) is not allowed in school.

- Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.

- Do not attempt to visit websites that may be considered inappropriate or illegal. Downloading some material is illegal and the police or other authorities may be called to investigate.

- The school's ICT Manager automatically monitors all Internet usage so you are responsible for all Internet sites accessed under your login as this information is recorded for compliance purposes.

6.8 Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time using their own computer at home. 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 must 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', nor invite them to be friends with you.

- You must ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.

- You should avoid contacting any pupil privately via social networking site, 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 to access to your personal information.

It is advised not to accept invitations from the pupils' parents or carers to add me as a friend to their social networking sites, nor should you invite them to be your friends. As damage to professional reputations can inadvertently be caused by quite innocent postings or images. You will need to ensure that any private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in anyway.

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 comments 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.

6.9 Use of your own Equipment

- 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.

- You must not connect personal computer equipment to school computer equipment without prior approval from the ICT Manager, without the exception of storage devices such as USB memory sticks.

6.11 Mobile Devices

No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from a member of staff.

Mobile phones

- Personal mobile phones should not be used in areas of school where pupils have access.

- During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard or locker away from the children.

- Adult are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room or teachers room (safe, suitable places where the children are not present).

- It is forbidden to take photographs/videos of the children on personal mobile phones.

Digital cameras

The school encourages the use of digital cameras and video equipment; however, staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name.

- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones.

- All photos should be downloaded to the school network

- The use of mobile phones for taking photos of pupils is not permitted.

6.12 Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment. Supervising staff needs to ensure that pupils have signed the class computer log and if the pupils are unable to sign the log book they are responsible for doing it for them. When arranging use of computer facilities for pupils, you must ensure supervision is available.

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

- 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.

6.13 Reporting Problems with the Computer System

It is the job of the ICT Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- You should report any problems that need attention to the ICT Manager.

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

- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the less chances of your data being recoverable.

6.14 Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the ICT Manager, School Business Manager or the Head Teacher, 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 pupil 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.

All reports will be treated confidentially.

6.15 Electronic Devices - Searching & Deletion

In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

7 Remote or Mobile Working

Remote or mobile working requires a higher degree of care as the risk to information is greater.

8 Lost or Stolen Assets

If school information is lost or stolen in the UK or abroad, due to a burglary or street robbery, you **must** report this to the SBM, Rachel Banks and the ICT Manager, Kevin Crouch, so that it is logged as lost or stolen.

The Information Governance Lead **must** be notified of losses if data stored on the device is of a personal, sensitive nature i.e. classified as OFFICIAL or higher. Or data has been lost in addition to that stored on the device.

9 Return of School Assets

All users, issued with computer equipment **must** return all assets upon termination of their employment, contract or agreement. This includes any removable storage media, laptops, mobile phones, tablets, software, computers, printers and any other computer equipment for home or mobile working.

Managers shall ensure that their staff return all equipment as part of the exit procedures, and notify the ICT Manager, kevin Crouch, so that their accounts are closed. All equipment shall be returned to IT for reallocation.

10 Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff. Our Acceptable Use Policy (AUP) has been created by our school governors and senior managers and approved by the whole school community.