

Billingham Church of England Primary School

ICT Acceptable Use Policy

Document Control

Date	Nov 2019
Version Number	V2.0
Author	R Allen
Approved by	

Contents

Aim	2
Scope	2
Training and Awareness	2
General Responsibilities	2
Unacceptable Use.....	2
Internet Use	3
Email	4
Passwords	5
Removable Media	6
Remote/Mobile Working.....	6
Personal Use of School ICT	6
Images and Video	7
Use of Personal ICT	7
Reporting Security Incidents.....	7
Monitoring	7
Disclosure of Data	7
Further Information.....	8
Review	8

Aim

The aim of this policy is to set out individual responsibilities which assist Billingham Church of England Primary School (the school) in protecting its Information and Communication Technology (ICT).

It supports the school's Information Security Policy.

Scope

The policy applies to:

- Any individual using or accessing school ICT;
- School owned or leased ICT such as PC's; laptops; notebooks; smart phones; software; services, storage media and network resources.

Training and Awareness

You must undertake information security and data protection training on a regular basis.

General Responsibilities

You must protect your user name, password, and security token (if used) against misuse.

All ICT must be subject to access control to ensure only authorised persons can access the ICT.

You must operate a clear screen policy when you leave your device unattended e.g. locking your computer by pressing the Windows key and the 'L' key simultaneously or by engaging the lock screen on your smartphone.

You must protect portable devices and removable media at all times. When not in use they must be subject to appropriate security e.g. placed out of sight under lock and key.

You must ensure all portable ICT used to store or process sensitive information, such as personal data, is encrypted.

You must ensure all ICT is returned to the Headteacher who will return it to the F1 Group when no longer required. This is to ensure devices are securely wiped or destroyed.

You must only access or attempt to access ICT that you have been authorised to access.

You must only access or attempt to access information for official school purposes aligned with your role and this must be on a need to know basis.

Unacceptable Use

You must not use the username and password of another person or share your own username and password with another person.

You must not misuse, bypass or change the configuration or security settings of any ICT.

You must not introduce unauthorised software, hardware, or removable media.

You must not process or access racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material.

You must not carry out illegal, fraudulent or malicious activity.

You must not use school ICT to carry out or support business which is unrelated to the school.

You must not break copyright or carry out any activity that negatively impacts intellectual property rights.

Internet Use

Use of the Internet is encouraged where such use supports the school's objectives.

You must not use the Internet to visit websites or post comments, remarks or any other material that could be construed as racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate.

It is recognised that under certain circumstances inadvertent access may happen, however such occurrences must be treated as an e-safety incident. Should you or a student access any of these sites unintentionally you should report the matter to the e-Safety Officer (Mrs Pool) so that it can be logged. In the case of the e-Safety Officer, she would report the matter to the Headteacher.

Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

You must not download electronic files or software without authority from the Headteacher.

You must not use the Internet to illegally share, reuse, or copy materials which are copyrighted and/or licensed.

Personal use of the Internet must be reasonable, proportionate and occasional.

Social networking – is blocked in our school.

Social Networking is not allowed at Billingham Church of England Primary School either by staff or pupils.

Members of staff should *never knowingly become* “friends” with students or parents on any social networking site or engage with pupils on internet chat.

If a member of staff is already ‘friends’ with a parent due to a historic friendship or a member of staff then they must not discuss/comment on anything associated with school on a social networking site.

If a member of staff accesses a comment from a social networking site that is inappropriate regarding Billingham Church of England Primary School then they should print it off and report it to the HT or the e-safety officer.

Email

All members of staff should use their professional email address for conducting school business. Any email that is used for official business (containing personal or sensitive data) must be sent from your official school domain address and not from your own personal email domain. Staff are not permitted to use school email addresses for personal/social use. You must not use personally owned email accounts to conduct school business or to transmit or receive school information.

Remember that all school email is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public. Although you may have deleted your copy of the email, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act and the General Data Protection Regulation.

Don't use email to store information which should be stored somewhere else. All attachments should be saved on an appropriate electronic filing system or printed out and placed on paper file.

As the employer, school has the right to monitor the use of email and this is something that we may do. Any monitoring will be carried out by Mr Allen.

School has migrated email to Office 365. School staff must use Office 365 to send and receive emails using their school email account. Staff can access email from school at home provided they use their encrypted laptop at home. Office 365 gives us encrypted email. You can access documents from home and save to One Drive as long as it is through your school provided encrypted laptop only. All file attachments to an email must be encrypted if personal data is included in the attachment. So what is personal data under GDPR? Personal data' means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier. Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

You can access school emails on phones and tablets as long as it has been provided by school and it has to be secure, password or key locked.

Ensure that when sending an email it is clearly written:

- Do not use text language or informal language in school emails.
- Always sign off with a name (and contact details).
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Always spell check an email before sending it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.

Do not write a whole email in capital letters. This can be interpreted as shouting

You must check that the recipients of e-mail are correct to avoid accidental release to unintended recipients. Particular care must be taken when using auto complete in your email client as an unintended email address may be used in error.

You must take care when opening an attachment or clicking on any link within any email unless you are confident the email is legitimate.

Suspicious email should be deleted and must not be forwarded to other recipients.

If you suspect an email contains malware please contact Mrs Pool or Mr Allen who will contact the F1 Group.

When sending an email to more than one recipient and it is necessary to protect email addresses the blind carbon copy (BCC) feature must be used.

When sending sensitive information via email you must ensure it is done so securely. This is achieved by using your Office 365 email account.

Personal use of school email shall be reasonable, proportionate and occasional and must not interfere with the performance of your role or the performance of the system.

Delegate access to email accounts must only be provided following a clear business need and only when authority is provided by the email account owner, or in their absence, the Head Teacher. To arrange delegate access please contact Mr Allen.

Delegate access must not be provided by supplying details of a User's credentials i.e. username and password.

When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must not open it or stop immediately if the email has been opened.

Passwords

Passwords must not be shared and must be protected from unauthorised disclosure.

When creating a passwords ensure it is not easily guessable e.g. 'letmein123', 'Password1' and avoid using keyboard patterns or sequential numbers e.g. qwerty, 12345.

Passwords must be a minimum of 8 characters in length and must contain upper and lower case letters, numbers and characters.

Passwords must not be recorded unless it is done so securely and you are the only one who can access it.

The same password must not be used across different accounts (work and private) and/or applications. Passwords should be changed every 30 days.

Default passwords must be changed.

On no account should staff allow a pupil to use a staff log in.

Removable Media

Removable media which contains sensitive information such as personal data must be encrypted. Removable media includes USB flash drives, CDR, DVDR, removable hard drives. Please question yourself – is it really necessary to take it home? Does it have to be on a USB memory stick. If so then you must only use your encrypted password protected USB stick provided by school. Can you use secure cloud storage (One Drive) on Office 365 instead?

Removable media from an unknown source must not be introduced to school ICT as it may contain malware designed to harm school systems.

Remote/Mobile Working

Additional care must be taken when working outside of school premises and you must ensure that reasonable safeguards are taken to manage the increased likelihood of a security incident.

You must only remove ICT from school premises when there is a clear business need.

You must prevent inadvertent disclosure of information and avoid being overlooked when working.

When removing ICT from school premises, and it contains sensitive information such as personal data, only do so if it is encrypted.

You must avoid storing ICT in an unoccupied vehicle unless more secure options are unavailable. If it is unavoidable then you must place the ICT out of sight, in the locked boot of the vehicle.

ICT must never be stored in a vehicle overnight.

Portable devices must connect to the school's ICT network on at least a monthly basis in order to receive security updates. You must ensure devices remain connected until such time updates have been received and applied i.e. Windows updates.

Staff can only use laptops purchased by school to hold/ store personal data (about pupils, parents/carers and staff) as these will be encrypted along with password protection. Staff cannot use their own laptop/PC to hold any personal data. If it currently does, then it will have to be deleted. Any school information held on your school issued encrypted laptop or memory stick cannot be transferred to a privately owned device.

Ipads and storage of photos. Please make sure that any photos taken on an iPad are deleted from the device once uploaded. They should be uploaded to the server as soon as possible after the photo is taken. Photos that identify children should not be kept on an iPad. Staff should only use their iPad provided by school and must ensure it is password protected. No personal data / information should be stored on it.

Personal Use of School ICT - Staff are not permitted to use school owned ICT equipment for personal use unless specific permission has been given from the Headteacher who will set out the boundaries of acceptance. Staff are able to use their school iPads and laptops for personal use as long as all the points in this policy are adhered to.

Images and Videos - Staff and pupils should not upload onto any internet site or service images or videos of themselves or other staff or pupils without consent. This is applicable professionally (in school) and personally (i.e. staff outings).

Use of Personal ICT – staff are not permitted to use their personal ICT equipment in school. This includes the use their own personal devices (such as mobile phones or tablets etc) to take photos of children for example at events in school or out of school (e.g. sporting events). School ipads or the school camera should be used for such photos.

Reporting Security Incidents

All security incidents and suspected security incidents must be reported in accordance with the school's Security Incident Policy.

If you identify suspicious activity while using ICT or believe that you are the victim of malware e.g. a virus you must stop what you are doing, power off your ICT and report it immediately.

You must report all security incidents to the Headteacher.

Monitoring

The school reserves the right to monitor its communication systems and services.

This includes, but is not limited to, email, telephone conversations, electronic messaging, internet use, and system access.

Monitoring is used by the school for the following purposes:

- To maintain and ensure security of systems and information;
- To check for unauthorised use;
- To establish facts relevant to school business;
- To ensure quality assurance and ensure that procedures are being followed;
- To undertake disciplinary, performance, and capability proceedings; and
- To prevent or detect crime.

Disclosure of Data

Please ensure and be aware of the importance of ensuring that personal data / information is only disclosed to people who are entitled to receive it. Personal data processed must be adequate, relevant and limited to what is necessary (for purpose it was intended/collected for). Do not hold copies of personal data if it is sufficient to only retain a record that it exists. Personal data should not be kept for any longer than is necessary. See the Retention and Disposal Schedule – IRMS - as part of the school's Asset Register. All staff must ensure personal data is secure and must protect against unauthorised or unlawful processing, accidental loss or damage or deliberate loss.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such all staff will promote positive e-safety messages in all use of ICT whether with other members of staff or with pupils.

All staff are to sign the attached sheet stating that they have received and read this policy and will comply with its contents. **Staff thereby accept that the school can monitor network and internet usage (including e-mail) to help ensure staff and pupil safety.**

If there is any suspicion of illegal activity staff should never investigate themselves but must report to Lincolnshire Police as soon as possible.

Any member of staff who flouts security advice or uses ICT technology for inappropriate reasons risks dismissal.

Further Information

For further information regarding ICT acceptable use within the school please contact:

Michelle Hall
Data Protection Officer
michelle.hall@billinghay.lincs.sch.uk
01526 860786

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

Review

This policy shall be reviewed annually.