IT Authorised Acceptable Use Policy Staff, Governors & Volunteers

Date adopted by Governing Body ……

Signed on behalf of the Governing Body ……

Name in block ……..

Review Date……Autumn 2020……..

Why have an Authorised Acceptable Use Policy?

An Authorised Acceptable Use Policy is about ensuring that you, as a member of staff/volunteer/School Governor at Battling Brook Primary School can use the Internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet and email, managed learning environment and websites.

An Authorised Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore **fraud**. Also that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. We have also banned certain sites which put the school network at risk.
Help us, to help you, keep safe.

Battling Brook Primary School strongly believes in the educational value of ICT and recognises its potential to enable staff and volunteers in delivering and supporting the curriculum. Battling Brook Primary School also believes that it has a responsibility to educate its pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and other related technologies. To this end the expectation of Battling Brook Primary School is that both staff and volunteers will play an active role in implementing school and departmental Internet safety polices through effective classroom practice.

Battling Brook Primary School recognises that for staff and volunteers to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the School and have the opportunity to expand and develop the teaching material associated with their work. However, Battling Brook Primary School expects that both staff and volunteers, will at all times, maintain an appropriate level of professional conduct in their own use of the School's ICT facilities.

Listed below are the terms of this agreement. Staff, School Governors and volunteers are expected to use the ICT facilities of the School in accordance with these terms. Violation of these terms is likely to result in disciplinary action in accordance with Leicestershire County Council Disciplinary Procedures for Local Government Services Employees. Where the policy is breached in by either volunteers or governors the School will seek to advice and support from the Local Authority in order to manage the situation in a fashion that safeguards the school population.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein.

1. Equipment

1.1 School Computers

All computers and associated equipment are the property of Battling Brook Primary School and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990 (plus amendments), and the General Data Protection Regulations (see Glossary). The School assumes responsibility of maintenance of all hardware and software. Mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware
- Deliberate deletion of files.
- The uploading of non-work based computer files to the School's network

Any of these actions reduces the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

1.2 Laptop Computers

Laptop computers are issued to all teaching staff and support staff as required. Laptops remain the property of Battling Brook Primary School all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Battling Brook Primary School at all times and must be returned to the School at the discretion of the Headteacher.
- Maintenance of the equipment is the responsibility of the Battling Brook Primary School. All maintenance issues must be referred to the ICT network manager R Kotecha through the usual channels.
- Accidental damage/loss to laptops must be repaired/replaced at the user's own cost unless covered by warranty.
- All installed software MUST be covered by a valid license agreement held by Battling Brook Primary School.
- All software installation MUST be carried out by R Kotecha or the school's nominated software specialist in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. *This should be done frequently within a cycle programme of no longer than 12 months.*.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up to the Battling Brook Primary School network. Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network. It is recommended that the school's facility to transfer files is used.
- The user of the equipment must not encrypt <u>any</u> data or password protect the laptop/files so as to ensure future usage of the equipment.
- Battling Brook Primary School cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for R Kotecha or the school's nominated software specialist to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

1.3 Use of Removable Storage Media

Staff must not use CD disks or flash memory devices to transfer files between home and school, this must be undertaken via email facilities. Battling Brook Primary School Battling Brook Primary School cannot guarantee the correct operation of any removable media device or the integrity of the data stored on it. It should be noted that rewriteable CDs in particular are neither robust nor reliable, and should not be used as a means of storage for important files. Battling Brook Primary School cannot guarantee the correct operation of flash memory devices, although every effort is made to ensure that this facility is available. Staff must not transfer any files containing confidential material between home and school <u>via the web</u> to ensure security integrity in accordance with the General Data Protection Regulations. All documents with sensitive information must be attached as files and password protected.

1.4 Printers and Consumables

Printers are provided across the School for educational or work-related use only. All printer usage can be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential
- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.

1.5 Data Security and Retention

All data stored on the Battling Brook Primary School network is backed up for a limited period. If you should accidentally delete a file or files in your folder or shared area, please inform R Kotecha. Generally, it is not possible to recover files that were deleted but every effort will be made if deemed necessary.

2. Internet and Email

2.1 Content Filtering

Battling Brook Primary School provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report these to R Kotecha so that they can be blocked or filtered.

2.2 Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the School. This includes abiding by copyright laws.
- Do not access Internet chat sites. These represent a significant security threat to the School's network.
- The use of online gaming sites is prohibited. These consume valuable network resources that may adversely affect the performance of the system.
- Do not print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.
- Do not attempt to download or install software from the Internet including apps. R Kotecha assumes responsibility for all software upgrades and installations.
- Staff are reminded that ALL Internet access is logged and actively monitored and traceable.

2.3 Email

Staff, where necessary are provided with an email address by Battling Brook Primary School. This may be used for any legitimate educational or work-related activity. Staff should use the email in accordance with the following guidelines and are reminded that the School retains the right to monitor email communications at any time if this is deemed necessary.

The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.

- Messages relating to, or in support of any illegal activities may be reported to the authorities.

- Whilst it is possible to attach files to an email message, staff are advised that that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 5MByte in size are generally considered to be excessively large and staff should consider using other methods to transfer such files.

- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the School network.

- Staff should not send personally identifiable information by email, as it is not a secure medium. Data must be kept to a minimum in order to not identify a single individual and should be within an attached password protected document.

3. External Services

Battling Brook Primary School provides a number of services that are accessible externally, using any computer with an Internet connection. These should be used strictly for educational or work-related activities only and in accordance with the following guidelines

3.1 Web-Email

Web email provides remote access to your email account from home or anywhere with an Internet connection. Use of this service is subject to the following guidelines. Staff should use email in accordance with the following guidelines and are reminded that the Battling Brook Primary School retains the right to monitor email communications at any time if this is deemed necessary.

- Web-email is provided for use of Battling Brook Primary School staff and students only. Access by any other party is strictly prohibited.

- By using Web-Email, you signify that you are an employee of Battling Brook Primary School, and that you have been authorised to use the system by the relevant School authority.

- Observe security guidelines at all times. Never reveal your password to anyone. If you are unsure that your password has been shared to a third party, change the password immediately.

- Remember to treat incoming file attachments with caution. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Battling Brook Primary School accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

- The rules that apply to Email are also to Web-Email.

4.0 Privacy and Data Protection

4.1 Passwords

- Never tell your password to anyone.
- Never display your password so that it is visible to others or ask others for their password.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.
- If you forget your password, please request that it be reset via R Kotecha.
- If you believe that a student or other staff may have discovered your password, then change it ***immediately***.

4.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.
- If you believe a data breach may have occurred you must report any security concerns immediately R Kotecha and S Marsden (Headteacher).
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with the school's Disciplinary Procedures.

5.0 Management and Information Systems

Access to MIS software is available only from designated locations and only to those staff who require it. Access is subject to agreement with the Headteacher, Business Manager and/or R Kotecha. Usage of MIS software is subject to the following guidelines:

- Password security is vital. If you believe that your password has been discovered by a student or other member of staff, **change it immediately**.
- Computers unattended, particularly in a classroom, must either be log out or locked by using the CTRL-ALT-Delete keys and then choosing "Lock Workstation". Once this is done, you will need to re-enter your password to gain access to the computer.
- If you are using MIS software on a computer in a classroom connected to an interactive whiteboard and projector, please be aware that any student information you display on your screen may also be displayed on the whiteboard if the projector is turned on. To ensure protection of sensitive data, pleas ensure that projectors are turned off or disconnected before using MIS software.
- Joining administration and curriculum networks raises issues regarding who within the school organisation has access to data. Within Battling Brook Primary School it is understood that the Headteacher and Senior Leadership team have a clear duty of care to protect the access to confidential data. Further details

regarding this aspect of the School's E-safety approach can be found in Appendix G (Management and Information Systems).

6.0 Mobile Technologies

Please refer to the schools Mobile Phone Policy.
For reasons of safety and security staff, governors and volunteers must not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 3G and 4G mobile phones also means that adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

In order to reduce the opportunity for those behaviours that could possibly cause upset, it is requested that staff, governors and volunteers working with children and young people within the school setting, limit their use of mobile technologies to necessary communication during specified breaks in non-teaching areas during the school day.

If you are sent inappropriate material e.g. images or videos **report it immediately to the Headteacher**.

7.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to R Kotecha or the school's chosen IT specialist using one of the following methods:

- Telephone LEAMIS 0116 2311280
- Email rikin@bbrook.leics.sch.uk
- In person at the ICT suite

Battling Brook Primary School will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

7.1 Software Installation

R Kotecha assumes responsibility for all software installation and upgrades. Staff may request the installation of new software packages onto the network, but this will be subject to the following:

- Software cannot be installed on the School's network without a valid license agreement. This must be supplied with the software package.
- Please check the licensing terms of the software package carefully to ensure that it is suitable for use. If you are unsure, please ask R Kotecha for assistance or contact the software supplier. A relevant and valid license agreement document will be required before any software packages can be installed.
- All software installation media and license agreements are held centrally within the School to aid in license tracking and auditing. Installation media cannot normally be released except by special agreement.
- No member of staff is allowed to purchase software for use on the School network other than the IT Network Manager (R Kotecha). Purchase orders for new software will normally be authorised only with the agreement of the Business Manager.

7.2 Service Availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the School will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the School ICT system is at your own risk. Battling Brook Primary School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

Glossary

- Computer Misuse Act

  The Computer Misuse Act makes it an offence for anyone to have:-

  - Unauthorised access to computer material e.g. if you find or guess another user's password and use it.
  - Unauthorised access to deliberately commit an unlawful act e.g. if you guess another user's password and access their learning account without permission
  - Unauthorised access with intent to commit or facilitate commission of further offences
  - Unauthorised access to change computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.
  - Unauthorised access to commit acts with intent to impair, or with recklessness as to impairing, operation of computer
  - Unauthorised access to make, supply or obtaining articles for use in an offence

- General Data Protection Regulations 2018

  The General Data Protection Regulations ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school.

  The Regulations cover the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Regulation not only applies to paper files it also applies to electronic files.

  The Principles of the Regulations state that data must be:

  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Kept no longer than necessary
  - Processed in accordance with data subject's rights
  - Secure
  - Not transferred to other countries without adequate protection

- RIPA – Regulation of Investigatory Powers Act 2002
  If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:
  - the interception of communications
  - the acquisition and disclosure of data relating to communications
  - the carrying out of surveillance
  - the use of covert human intelligence sources

- access to electronic data protected by encryption or passwords

If a request for authorised access is made to the school, we will provide the appropriate access to your ICT records and files.

REQUIRED SIGNATURE - MEMBER OF STAFF/VOLUNTEER

I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to the R Kotecha or the Headteacher. I agree to use the Internet and electronic communications systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.

Name ***Signature*** ***Date***