John Wycliffe Primary School

Policy:	E-SAFETY POLICY
Date Agreed:	27th January 2014
Term/Year to be reviewed:	Summer Term 2016
Sub-Committee to review:	Curriculum & Standards

1. Introduction

1.1 John Wycliffe Primary School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at John Wycliffe Primary School want to ensure that new technologies are used to raise standards by developing the curriculum thus making learning exciting and purposeful. Pupils learn in a way that ensures their safety and security is ensured. Pupil's lives and understanding are enhanced and enriched.

1.3 We are committed to an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give less abled pupils increased access to the curriculum to enhance their learning.

1.4 We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, is informed about the risks that exist so that they can take an active part in safeguarding children.

1.5 The nominated senior person for the implementation of the School's E-Safety policy is Vickie Njoroge - Headteacher.

2. Scope of Policy

2.1 The policy applies to:-

- All pupils;
- All teaching and support staff (including peripatetic), school governors and volunteers;
- All aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 John Wycliffe Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:-

- A list of authorised persons who have various responsibilities for E-safety;
- A range of policies including acceptable use policies that are frequently reviewed and updated;

- Information to parents that highlights safe practice for children and young people when using new technologies;
- Audit and training for all staff and volunteers;
- Close supervision of pupils when using new technologies;
- Education that is aimed at ensuring safe and responsible use of new technologies;
- A monitoring and reporting procedure for abuse and misuse.

3 Infrastructure and Technology

3.1 Partnership working

3.1.1 John Wycliffe Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the East Midlands Public Sector Network (emPSN) who provides a managed (not 'locked down') network system. We fully support and will continue to work with emPSN to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures.

3.1.3 We work with our partners and other providers to ensure that any pupils who receive part of their education away from school are e-safe.

4. Policies and Procedures

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils. We systematically review and develop our e-safety policies and procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of pupils and families to assist us in developing our e-safety policies and procedures.

4.1 Use of new technologies

4.1.1 We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 John Wycliffe Primary School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Users are not allowed to:-

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children;
- Promoting discrimination of any kind;
- Promoting racial or religious hatred;
- Promoting illegal acts;
- Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e. cyber bullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material.

4.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:-

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative);
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist or anti-religious material;
- Violence and bomb making;
- Illegal taking or promotion of drugs;

[1] For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

- Software piracy;
- Other criminal activity.

4.1.5 Additionally, users are not allowed to:-

- Use the emPSN or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves emPSN or member Local Authorities in any way;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of emPSN, or to emPSN itself;
- Visit sites that might be defamatory or incur liability on the part of emPSN or member Local Authorities or adversely impact on the image of emPSN;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:-
  financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;
- Assist with unauthorised access to facilities or services accessible via emPSN;
- Undertake activities with any of the following characteristics:-
  - Wasting staff effort or networked resources, including time on end systems accessible via the emPSN network and the effort of staff involved in support of those systems;
  - Corrupting or destroying other users' data;
  - Violating the privacy of other users;
  - Disrupting the work of other users;
  - Using the emPSN network in a way that denies service to other

users (for example, deliberate or reckless overloading of access links or of switching equipment);
- Continuing to use an item of networking software or hardware after emPSN has requested that use cease because it is causing disruption to the correct functioning of emPSN;
- Other misuse of the emPSN network, such as introduction of viruses;
- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

4.1.6 Where KCOM and Capita (providers of Internet connectivity and associated services to schools) and/or emPSN become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

4.2.1 There may be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately. (Refer to Appendix E).

4.2.2 The School also recognises that there may be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB[2] Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

5.1 John Wycliffe Primary School recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

5.2 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

5.3 To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship;
- Audit the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies;
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety policies and procedures.

6. Standards and Inspection

John Wycliffe Primary School recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use.

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, John Wycliffe Primary School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

[2] Chapter 9 of the LSCB Procedures

[3] Chapters 5, 9, 12 and 13 of the LSCB Procedures

6.1.3 We will also monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

6.2.1 We will support pupils and staff as necessary in the event of a policy breach.

6.2.2 Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

- **Child / Young Person**
  - The child/young person will be disciplined according to the behaviour policy of the school;
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- **Adult (Staff and Volunteers)**
  - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy;
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to Mrs Butcher – ICT Technician so this can be recorded for monitoring purposes.

7. Working in Partnership with Parents and Carers

7.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We also appreciate that there may be some parents who are concerned about the use of the new technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

Appendix A: ICT AUP – Staff, Volunteers and Governors
Appendix B: ICT AUP - Pupils
Appendix C: Personal Use of Social Media Sites Policy
Appendix D: Information Security Policy
Appendix E: E-Safety Incident Log Form
Appendix F: List of authorised persons

Appendix A

ICT Acceptable Use Policy (AUP)
(Staff, Volunteers and Governors)

Why have an ICT Authorised Acceptable Use Policy?

An ICT Authorised Acceptable Use Policy is about ensuring that you, as a member of staff, volunteer or governor at John Wycliffe 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 ICT 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.

John Wycliffe 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. John Wycliffe 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 John Wycliffe 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.

John Wycliffe 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, John Wycliffe 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 John Wycliffe Primary School and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990 and the Data Protection Act 1998 (see Glossary). The School assumes responsibility of maintenance of all hardware and software. Misuse 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 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

Laptops remain the property of John Wycliffe Primary School all times, and their usage is subject to the following guidelines.

- The equipment remains the property of John Wycliffe Primary School at all times;
- Maintenance of the equipment is the responsibility of John Wycliffe Primary School. All maintenance issues must be referred to the ICT Technician, through the usual channels;

- All installed software MUST be covered by a valid license agreement held by John Wycliffe Primary School;
- All software installation MUST be carried out by the ICT Technician or by a third party following consultation with the ICT Technician 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;
- 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, either to a CDRW disk, a memory stick, and external hard drive or to the John Wycliffe 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 any data or password protect any files so as to ensure future usage of the equipment;
- John Wycliffe 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 the ICT Technician 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

Whilst staff may use CD disks or flash memory devices to transfer files between home and school, John Wycliffe Primary School cannot guarantee the correct operation of any removable media or the integrity of any data stored on it. It should be noted that rewriteable CDs in particular are neither robust nor reliable, and should not be used as the sole means of storage for important files. John Wycliffe Primary School cannot guarantee the correct operation of flash memory devices on the system, although every effort is made to ensure that this facility is available.

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.

- 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 John Wycliffe Primary School network is backed up daily and backups are stored for up to 7 days. If you should accidentally delete a file or files in your folder or shared area, please inform the ICT Technician immediately so that a recovery attempt can be made. Generally, it is not possible to recover files that were deleted more than 7 days previously.

2 Internet and Email

2.1 Content Filtering

John Wycliffe 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 the ICT Technician so that they can be 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. The ICT Technician 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 are provided with an email address by John Wycliffe 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 it 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 5Mb 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.

2.4 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 School retains the right to monitor email communications at any time if this is deemed necessary.

- Web-email is provided for use of John Wycliffe 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 John Wycliffe 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;
- Remember to treat 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. John Wycliffe 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.

3 Privacy and Data Protection

3.1 Passwords

- Never reveal your password to anyone else 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 by consulting with the ICT Technician;
- If you believe that a student or other staff may have discovered your password, then contact the ICT Technician about your concerns **immediately**.

3.2 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;
- You should report any security concerns immediately to the ICT Technician;
- Any user identified as a security risk will be denied access to the system and could be subject to disciplinary action.

For reasons of safety and security staff, governors and volunteers should 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. In addition, the use of a personally owned mobile phone or PDA to record still or moving images of children or young people within the school setting is prohibited.

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/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 advisable 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 during the school day.

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

4 Support Services

All ICT hardware and software maintenance and support requests should be submitted to the ICT Technician using one of the following methods:

Email: sbutcher@johnwycliffe.leics.sch.uk

In person at school by logging a request within the ICT Maintenance/ Request Log Book.

5. Software Installation

The ICT Technician 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:

- A minimum of one week is required for unpackaging and installation of new software;
- Software cannot be installed on the John Wycliffe Primary School 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 on the School network. If you are unsure, please ask the ICT Technician 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 John Wycliffe Primary School to aid in license

tracking and auditing. Installation media cannot normally be released except by special agreement;

- When purchasing new software for use on the school network, please check its suitability, compatibility and licensing terms with the ICT Technician. Purchase orders for new software will normally be authorised only with the agreement of the ICT Technician and Headteacher.

6. 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 John Wycliffe Primary School ICT system is at your own risk. John Wycliffe 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 changes to 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.

Data Protection Act 1998

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school. The Act covers the collection, storing, editing, retrieving, disclosure,

archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

The Principles of the Act 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

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/GOVERNOR

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 ICT Technician 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_____

Appendix B

ICT Acceptable Use Policy (AUP)
(Primary Pupils)

John Wycliffe Primary School recognises the importance of ICT in education and the needs of pupils to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for pupils to use for their studies. To allow for this John Wycliffe Primary School requires all pupils' parents to sign a copy of the Acceptable Usage Policy **before** they use the School's ICT facilities.

Listed below are the terms of this agreement. All pupils at John Wycliffe Primary School are expected to use the ICT facilities in accordance with these terms. **Please read this document carefully** and sign and date it in order to indicate your acceptance of the Policy on your child's behalf. Access to the School's ICT facilities will only take place once this document has been signed.

It is important that your child understands the policy, so please ensure you take time to explain/ discuss this with them.

1. Equipment

1.1 Care of the equipment

All the children will look after all equipment and treat everything with respect. This includes, making sure that there is no:-

- Deliberate damage to computer hardware such a s monitors, hard drives, printers, keyboards, mice or other hardware and change or removal of software.

These actions make it difficult to ensure that the school is able to provide your child with reliable and available computer equipment and it has a cost implication for the school.

1.2 Printers

Printers are provided across the school for use by pupils. It is important that children learn to press the print key once and be patient.

2. Internet and Email

2.1 Content Filtering and use of the Internet

John Wycliffe Primary School provides two layers of internet filtering, designed to remove controversial, offensive or illegal material that would cause your child to be upset. The School makes use of the age-related filtering services provided by the East Midlands Public Sector Network (emPSN) which seeks to provide internet use that is safe and for educational purposes only.

2.2 Email

As part of your child's work in Information Technology and other subjects, we offer supervised access to the Internet and **internal** e-mail. On some occasions children are offered the opportunity to use e-mail outside the school, for example to communicate with children from other schools.

The Internet is a rich source of information and provides educational activities which are of great benefit to the children. However there are concerns about inappropriate materials and the school takes a range of measures to minimise these risks:-

- All access to the Internet is supervised by adults;
- A high level filtering system is in operation;
- Children are not allowed access to chat rooms or social networking sites at any time;
- Children are taught about safe Internet use by their teachers and via termly workshops by the ICT Technician.

All children have use of a generic 'year group' email address. It is important in all emails to:

- **Be Polite** - never send or encourage others to send abusive messages.
- **Use appropriate language**

3. External Services

3.1 Managed Learning Environment Software

MyMaths.co.uk provides a web-based portal allowing children access to personalised learning resources and lesson materials. Use of this

service should only be in accordance with instructions from the class teacher and in accordance with the following guidelines:

- MyMaths is provided for the use of John Wycliffe Primary School staff and pupils only. Access by any other party is strictly prohibited.
- Your child should never reveal his/her password to anyone or attempt to access the service using another pupil's login details.
- The remote access service is provided by MyMaths Limited (www.mymaths.co.uk) and John Wycliffe Primary School can make no guarantees as to service availability or quality.

4. Privacy and Data Protection

Children will be given a simple and an easy to remember network username/password which they will learn to use.

5. Mobile technologies

For reasons of safety and security your child should not use his/her mobile phone or any other technology in a way that is likely to damage the reputation of the school or risk the welfare of other pupils or adults that work within the school. If inappropriate material is sent to a pupil, it must be reported **immediately** to a member of staff within the school. Possession and use of a mobile phone by pupils and parents is not permitted during the school day. Where applicable, on arrival at school, pupils are requested to hand in their mobile to the school office for safekeeping and collect it at the end of the school day. Parents visiting the school premises are required to ensure that their mobile phone is turned off and safely secured on their person.

6. Service

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 John Wycliffe Primary School ICT system is at your own risk. John Wycliffe Primary School specifically denies any

responsibility for the accuracy of information obtained whilst using the ICT systems.

PARENTS / CARERS

I have read this ICT Acceptable Use Policy **and I have discussed this with my child**. I agree for my child: _____

Class: _____ to use the Internet and email in accordance with the school guidelines.

Signed: _____
Parent/Carer

Signed: _____
Pupil

Date: _____

Please return this slip to John Wycliffe Primary School immediately.

Please note that this document is included in the Permissions Booklet signed when a child starts school and also annually thereafter.

Appendix C

Personal Use of Social Media Sites Policy and Procedure

1 Policy and Procedure Approval

This model policy and procedure has been agreed with the recognised trade unions and is recommended by the Local Authority for adoption by all Leicestershire School Governing Bodies. Should, exceptionally, a governing body seek to amend this recommended document or adopt an alternative procedure, they will need to undertake formal consultation collectively with the County Secretaries of all the recognised trade unions for teaching and support staff. Any amendments or variations agreed should then be sent to the School HR Adviser as confirmation to the Local Authority. Governing bodies are strongly recommended to seek advice from the CYPS HR Team in these circumstances.

Agreed with Support Staff Trade Unions – 06/04/11 (subject to formal agreement.
Agreed with Teachers' Trade Unions/Associations – 17/03/11

2. Purpose

The primary purpose of the Personal Use of Social Media Sites Policy and Procedure is to clarify for employees how they should conduct themselves when using all forms of social media sites. If followed, it will help employees to minimise the risk they may unintentionally place themselves and pupils in when they choose to write about their work. This in turn will avoid situations where safeguarding concerns could arise, employees' integrity could be undermined, the School or the County Council brought into disrepute and professional relationships with colleagues and pupils compromised.

Additionally, adhering to the policy reduces the risk of employees inadvertently contravening sections of the Data Protection Act or falling foul of libel, defamation and copyright laws.

3. Scope

The policy is recommended for all employees in Schools.

This policy is concerned with the personal use of social media sites, not with work/official social media sites. Employees wanting to create a work-related social media site must discuss this with and obtain approval from the Head Teacher.

This policy should be read in conjunction with the Schools' Acceptable Use Policy.

4. Principles

- The School' commitment to equality of opportunity will be observed at all times during the operation of this procedure. This will ensure that employees are treated fairly and without discrimination on the grounds of race, nationality, ethnic or national origins, gender, marital status, disability, age, sexual orientation, trade union membership or activity, political or religious belief and unrelated criminal conviction.
- This policy is not intended to prevent employees from using social media sites, but to make them aware of the risks they could face when sharing information about their professional and/or personal life.
- Employees should be encouraged to report any concerns that they have regarding content placed by employees on social media sites. Employees should report their concerns to the Head Teacher.

5. Roles and Responsibilities

Line Managers	Head Teachers/Principals should ensure that all employees are aware of the Personal Use of Social Media Sites Policy and Procedure and of their responsibilities under it. It is the responsibility of the Head Teacher/Principal to ensure that breaches of the policy are investigated and addressed – this may include referral to the Local Authority's Safeguarding Unit.
Employees	Employees are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place children or vulnerable adults at risk, bring the School/College into disrepute or damage their own professional reputation.
HR Services	The CYPS HR team is available to advise and support Head Teachers/Principals on the application of the policy and procedure.
ICT Services	The ICT Services team is available to offer technical advice and support to Head Teachers/Principals when conducting an investigation.
Trade Union or other representative	Employees have the right to be accompanied at any formal meetings. The employee may be accompanied by: • A work colleague • A Trade Union representative.

6. Procedure

Social media sites covered

This procedure covers the use of all types of social media sites, which include but are not limited to:

- Social networking sites e.g. Facebook, MySpace and Instagram
- Blogging
- Micro blogging sites e.g. Twitter
- Video Clips and Podcasts e.g. You Tube
- Discussion forums.

Responsibilities of employees

- Employees are personally responsible for the content they publish on social media sites. Employees must be mindful that what is published will be public for a long time.
- To avoid any conflict of interest, employees should not normally request or accept pupils as "friends"; if in exceptional circumstances they wish to request or accept pupils as "friends" (e.g. where the pupil concerned is their son/daughter), the employee must seek guidance from their line manager first.
- Information must not be posted that would disclose the identity of pupils.
- Pupils must not be discussed on social media sites.
- Photographs or videos of pupils or their homes must not be posted on social media sites.
- Employees should not post information on sites, e.g. photographs and videos that could bring the School or the County Council into disrepute.
- Employees must not represent their own views/opinions as being those of the School or the County Council.
- Potentially disparaging remarks towards the School, the County Council, employees, pupils, pupils' relatives, Council suppliers and partner organisations should not be posted on social media sites.
- Employees must not either endorse or criticise service providers used by the School or the County Council or develop on-line relationships which create a conflict of interest.
- Employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive or discriminatory language on social media sites.
- Employees must not divulge any information that is confidential to the School, the County Council or a partner organisation.

Security

Employees should be mindful when placing information on social media sites that it is potentially visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for false allegations and threats. In addition it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security.

Furthermore there is the scope for causing offence or unintentionally causing embarrassment, for example if pupils find photographs of their teacher which may cause embarrassment and/or damage to their professional reputation and that of the School/College. In addition, it may be possible for other social media site users to identity where employees live, which could have implications for individual security.

Therefore, first and foremost consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above (see employee guidelines prepared by ICT Services at **Attachment 1**).

Employee groups / networks

Employee groups can be created on social media sites such as Facebook. Creators of these groups are responsible for monitoring the content of the site and ensuring that it is appropriate.

Disciplinary action

Employees should be aware that the use of social media sites in a manner contrary to this policy may result in disciplinary action.

Any instances of "cyber bullying" will initially be addressed under the Dignity at Work Policy and Procedure and may result in disciplinary action.

ATTACHMENT 1

Employee guidelines

1. Introduction

At the time of writing, there are over 250 million Facebook users around the world, making it the most popular social networking site. However, the use of social media sites like Facebook carries a great deal of risk. For example, Facebook profiles can often contain names, addresses and dates of birth. This can lead to anyone being able to set up a credit card in your name. Also, identity thieves would find it easier to piece together information about you from different websites/resources and use it to their advantage. This sounds unlikely but it is a real risk: the Press often carries stories about people who have lost money or had their credit rating damaged, which can be very tedious to correct.

Many employees are registered onto Facebook or similar websites such as Twitter. This guidance has been produced to help you, as an employee, ensure that correct privacy settings have been enabled within your Facebook profile. For other social networking sites, the same rules and risks apply in principle, so you are advised to become aware of what privacy settings are built into the site and take time to change the default settings.

2. Scope

This guidance document relates to all social networking websites including, but not limited to, Facebook, Instagram, Twitter and MySpace.

This document is not intended to encourage the use of Facebook or similar social networking sites, but rather to ensure that employees who use these websites are doing so safely.

3. Risks

There are many risks with using Facebook. Here are some risks that you need to be aware of:

- Anyone could find out information about you through the use of Facebook.
- Threatening messages could easily be sent through the use of

Facebook, in particular to those who have jobs within Adults and Communities, CYPS and Schools/Colleges, Trading Standards and Parking Fines.

- Risks to professionalism and independence when working with children and vulnerable service users.
- Information posted within the status field could possibly tell everyone that you are on holiday and your house will be empty for a couple of weeks.
- Risk to children who update their status to show their whereabouts.
- Possible damage to the School's or the County Council's reputation by posting inappropriate comments on another user's profile, which could be visible to everyone.
- Inappropriate photographs or offensive jokes posted on an employee's profile.

4. Facebook Privacy Overview

Facebook security is divided into the separate parts: (see figure 1)

- **Account Settings** – To controls username/password details and to control what information you share with others.
- **Privacy Settings** - Security settings within the website to control what information is visible on your profile e.g. basic information, personal information, photos, wall posts and searching.
- **Application Settings** - Security in relation to add on applications functionality e.g. events, groups, videos and gifts.

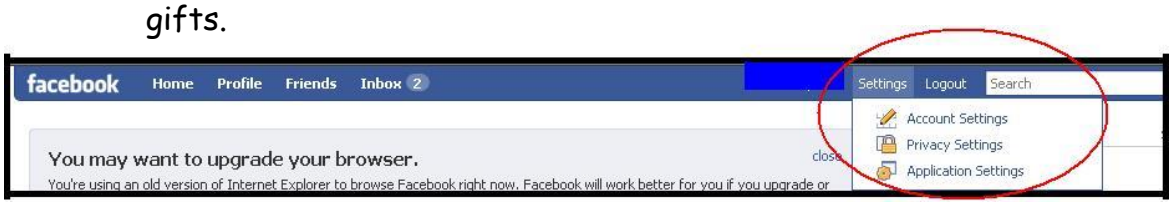

Figure 1

5. Account Settings

5.1 Information entered into your profile and accepting friends' requests

If you have entered your date of birth within your profile, change the privacy settings to display just the day and not the year.

Do not mention your mother's maiden name, your favourite pet or your school history in your profile. These are the security questions web sites such as banks use as part of checking who you are or in their "forgot password" functions. Although we recommend that you don't, some people use pet names and mother's maiden names as passwords, so by making this information available on your profile you may potentially be making it easier for people to hack your account.

If entering information or photos onto your profile, always bear in mind that a present or future employer could be viewing your profile.

Facebook provides every user with their own message board, also known as their "wall". The messages sent or received on your wall are displayed on your profile. Be careful about what is written on your wall and on your current status field, because others will be able to view the exchange of messages between you and your contact unless you secure your privacy settings (see Section 6 below for more information about privacy settings).

Examples of messages on user's wall which can be seen as a risk include:

- Telling your friends that you are going on holiday with the whole family – burglars would know there is an empty house and possibly your return date.
- Inviting your friends to a house party – this could lead to strangers inviting themselves along – this happened on a MySpace profile where a group of strangers turned up and caused thousands of pounds worth of damage to someone's house.

5.2 Accepting friend requests

Facebook encourages us to be friends with as many people as possible therefore some people may have a tendency to accept any friend requests they receive. As a Facebook user, you are advised to consider the following before accepting a friend's request:

- Think carefully about who you allow as a friend
- Remember people may not be who they say they are
- If in doubt of a person's identity, do not accept the request.

6. Security/privacy settings within the website

Facebook offers a wide range of privacy settings to control who you share your information with, but it is up to you to ensure that these controls are set at an appropriate level. It is important to explore all the options under the privacy heading and amend the ones you feel are relevant. When using any social networking website, never use the standard default privacy settings, as these are more likely to leave your account open for other users to view.

This section gives you further details of the main privacy settings available on Facebook and how they can help you control the way you share your information. Make time to view them all and decide on what level you wish to set them.

6.1 Profile

By default Facebook allows all your friends and networks (e.g. groups) to view your profile information. Networks can contain many thousands of people so you will be leaving your information visible to these users if you keep this on the default setting.

Facebook allows users to secure your profile using the privacy settings. There are three settings to choose from.

- **Making your profile available to everyone**
  This will make your profile available to everyone and anyone. This is not recommended.

- **Making your profile available to your friends and networks**
  This setting allows all your friends and networks to view your profile. Friends are usually the contacts that you have created/received a request from and will only appear on your contacts list when both users have clicked "accept".

  Your profile would be open to anyone else within your network, i.e. all the groups/networks that you have joined. Again this opens your profile to anyone else that's listed as a member.

- **Making your profile available to your friends only**
  This is the most secure option and is recommended. Other people can still search for you, but they would not be able to view your profile/photographs or comments until they are listed as a friend in your contacts list.

6.2 Search

You are able to change a setting within the privacy tab to stop people from finding your profile when they perform a search. The Facebook search facility makes it easy for anyone to enter your first name and/or surname into the search field and find a list of all the users on the site matching that name. Users are then able to sort within the results to narrow down the list of names more specifically by using other sorting options e.g. by locations, age, status, gender, location and many more.

The following settings can be changed in relation to searching:

Allow anyone to see my public search listing
If you want people you know to know that you are on Facebook, leave this unselected.

Allow my public search listing to be indexed by external search engine
If set to "yes", your details will be available via search engines such as Google and Bing.

If you allow others to search for your profile within Facebook, they will be able to do the following:

- See your profile pictures
- Send you a message
- Add you as a friend
- View your friend list
- If you haven't restricted your profile settings (see Section 5.1 above), the person who performed the search can view your profile fully.

6.3 Poke Messages and Friend Requests

Sending a poke, replying to a message or receiving a friend request temporarily allows that user to view your profile even if your normal privacy settings would not allow them to do so. This area allows you to control what profile information you wished to be visible. You should also be careful about who you reply to, if in any doubt you could block a user.

6.4 Block People

An option is available to block another user. They will not be able to search for you, view your profile or contact you on Facebook. Any current connections you have with that user will be removed (e.g. friendship, relationship). You can use this if you are having problems with a particular person trying to contact you.

7. Application Settings

Applications within Facebook include additional "add on" functionality, so for example, interest groups, games, events, videos etc.

You can edit the settings to allow or restrict the view of which applications you have added to your profile. You can customise this to allow selected friends to see which applications you have added but not all. The following options are available to choose from:-

- Everyone
- My network and friends
- Friends of friends
- Only friends
- Only me
- Customise.

Appendix D

Information Security Policy

1. Introduction

1.1 Information Security

The availability of complete and accurate information is key to providing excellent services to the pupils, parents and staff of Leicestershire schools. Leicestershire schools hold and process a large amount of confidential and personal information on private individuals, employees, service partners, suppliers and its own operation.

Leicestershire schools have a number of responsibilities to protect their reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore the **confidentiality**, **integrity**, **availability** and **accountability** of this information need to be protected from harm in a way that is proportionate to the risks to the information.

This Information Security Policy provides the overall framework to help everyone play his or her part in protecting pupil and staff information. It is consistent with Leicestershire County Council's corporate strategies on ICT and information management. This constitutes the high level policy.

This policy is supported by a comprehensive set of detailed policies, processes, procedures and guidelines, which constitute the Information Security Management Framework (ISMF).

A glossary of information security terms used in this policy is provided in Attachment 1.

1.2 Scope

The Information Security Policy applies to everyone who reads or processes school information. The policy applies **wherever** and **whenever** school information is processed and applies equally to **all users** including:

- Teachers, Governors, Teaching Assistants, Auxiliary Staff and Office Staff

- Contractors, consultants, casual and temporary employees and volunteers
- LA staff working on site (e.g. LEAMIS technicians, LA Group Bursar Service)
- Partners and suppliers

Please note that throughout this document, the words "employee" and "user" are used to cover all the groups of people listed above.

The Information Security Policy applies to **all forms of information**, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled by the Council, including information, which is:

- Spoken face to face, communicated by fixed line, by mobile telephone, or by two-way radio;
- Written on paper or printed out from a computer system. This may include working both on-site or remotely (e.g. at home);
- Stored in structured manual filing systems (see Attachment 1, Glossary of Terms);
- Transmitted by electronic mail, fax, over the Internet and via wireless technology;
- Stored and processed via computers, computer networks or mobile computing devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs);
- Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

1.3 Purpose

The purpose of the Information Security Policy is:

- To protect the School's Information and subsequently to protect the School's reputation
- To enable secure information sharing to deliver services
- To protect the School from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information

- To maintain awareness of information security
- To protect the School's employees
- NOT to constrain reasonable use of information in support of normal business activities of the School

This policy shall be seen as additional to all other school policies relating to information disclosure and personal conduct.

1.4 Breaches of the Information Security Policy

Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.

Breaches of this policy by a user who is not a direct employee of the School may result in action being taken against the user and/or their employer.

In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.

Breaches of the Data Protection Act 1998 could result in a hefty fine being issued to the individual and the organisation.

1.5 Legal Framework for Information Security

Line managers and individuals have responsibilities regarding the legal use of information. There are many laws and legal rules governing how information is handled. The list below demonstrates the importance of using information correctly.

- Common law in relation to duties of confidentiality
- Health and Safety at Work Act 1974
- Theft Act 1978
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
- Human Rights Act 1998
- Protection of Children Act 1999
- Freedom of Infomration Act 2000
- Computer Misuse Act 1990

This list is not exhaustive and will change over time. Users shall seek guidance about the legal constraints of using information in their work and the School, through the Council will provide appropriate guidance and training to its staff if requested.

1.6 Information Security Standards

The Information Security Policy and associated documentation is based on these British Standards, copies of which are held by Leicestershire County Council's Information Assurance Consultant:

- Information technology - Security techniques - Code of practice for information security management - (BS 7799-1:2005, also known as ISO/IEC 17799:2005)
- Information technology - Security techniques - Information security management systems - Requirements (BS 7799-2:2005, also known as ISO/IEC 27001:2005)

1.7 Further Information about Information Security

Further information can be found on the EIS Intranet or by contacting Katie Robey, Information and Policy Team Manager on 0116 30 55783 or email _ cypsinfosecurity@leics.gov.uk

2. Information Security Roles and Responsibilities

2.1 All Information Users

1. **Comply with** this Information Security Policy, processes, procedures and guidelines at all times.
2. Comply with legal, statutory, regulatory and contractual obligations related to information at all times.
3. Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to **confidentiality**, **integrity** and **availability**.
4. Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation.
5. Report immediately all suspected violations of this and all other security policies, system intrusions, and any other security incidents or weaknesses in security, which might jeopardise the School's information or information systems, following agreed incident management policies and processes. Attachment 3 of this document sets out who suspected violations should be

reported to. Where an individual feels that he/she is unable to report the issue to the head of establishment, he/she is reminded of the existence of the LA's Whistleblowing Policy, a copy of which is accessible in the School, which sets out additional avenues to report concerns, outside of the establishment itself.

6. Read and act on any communications and training about information security and ask for clarification if these are not understood.
7. Play an active role in protecting information in day-to-day work.

2.2 Governors and School Senior Leadership Team

1. Approve this high level Information Security Policy.
2. Actively promote effective and appropriate information security by the use of structured risk assessment in all future developments and by appropriate retrospective risk assessment of current processes and systems.
3. Implement and promote Information Security to all staff within their service areas.
4. Ensure that employees understand and abide by the Information Security Policy and its associated policies, processes, procedures, guidelines and understand its impact
5. Assign owners to all information in their area of responsibility
6. Provide effective means by which all staff can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.
7. Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
8. Provide written authorisation for access to information.
9. Ensure that communications regarding information security are cascaded effectively to all staff.
10. Ensure that information security is an integral part of all departmental processes.

2.3 Information owners

Data sets may have different owners and where several potential information owners exist, responsibility should be assigned to the manager whose group makes the greatest use of the data. For example, Office Managers, Bursars

1. Use structured risk assessment to select security controls to protect their information.
2. Monitor to ensure security controls continue to be effective and that information is being handled correctly.
3. Report and act on security incidents and weaknesses relating to their information according to agreed incident management policies and processes.
4. Manage the residual risks to their information.

5. Prepare appropriate Business Continuity plans and contingency arrangements.

2.4 ICT Services e.g. School Network Managers, LEAMIS etc

1. Be the custodian of electronic information in its care by implementing and administering technical security controls as specified in the information security policies, and by the Information Owners as a result of information security risk assessment.
2. Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
3. Assist schools to ensure all software is licensed and remove unlicensed software
4. Provide contingency arrangements for information systems
5. Provide appropriate protection from malicious software.
6. Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
7. Monitor and investigate technical security breaches.
8. Provide technical support to enable compliance with this policy.

2.5 CYPS Information Security Team

1. Provide agreed information security policies, processes, procedures and guidelines to assist the School in protecting information appropriately.
2. Provide training and consultancy in assessing information risk and selecting appropriate security controls.
3. Provide a library of materials demonstrating good practice to assist in structured information security risk assessment.
4. Promote awareness of information security throughout the Council and assist in ensuring that information security is an integral part of all departmental processes.
5. Liaise with information security specialists in other organisations, suppliers and industry analysts to maintain awareness of best practice in information security.

3. Compliance

3.1 The School operates within the law at all times.	1. Information shall be used legally at all times, complying with UK and European law. All users, including employees, and agents of the School might be held personally responsible for any breach of the law. 2. All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the Data Protection Act 1998. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation. 3. Advice shall be sought from CYPS Data Protection Representatives about what information is covered by the Data Protection Act and for detailed guidance about how to handle such information. 4. Personal, confidential or sensitive information **shall be protected** appropriately at all times and in particular when removed from School premises either physically on paper or electronic storage devices, or when transmitted electronically outside the School. 5. Personal, confidential or sensitive information shall not be included in the text of e-mails to be sent outside the authority, or in files attached to them, unless these are securely encrypted or sent by secure network links. Please be confident that the link is secure before this is used. 6. Any request for information under the Freedom of Information Act 2000 (FOIA) shall be handled in accordance with the law and processed within 20 working days. Anyone handling FOIA requests shall have completed the appropriate level of training. Where an exemption to FOIA might apply, further advice shall be obtained from Katie Robey, Systems Information Manager katie.robey@leics.gov.uk 7. Information shall not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others, Electronic and non-electronic communications shall not

	contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity. Note; It is accepted that in some professional situations such information is required for business reasons. 8. The School shall only use licensed software on its computers, servers and other computing devices such as personal digital assistants (PDAs). The School shall provide sufficient legally acquired software to meet all legitimate and agreed needs in a timely fashion. 9. Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of copyright.

3.2 Access to information shall be controlled.	The requirements for confidentiality, integrity, availability and accountability shall be determined for all information, from creation to deletion. 1. Structured information security risk assessment shall be used to determine the appropriate security controls required to protect information, which are proportionate to the risks to the information and information systems. This risk assessment shall be done as part of system and process development. The effort expended on risk assessment and the amount of formal documentation required shall be proportionate to the perceived risks to the information and the impact of a breach of its security. 2. Access to information shall be authorised by management, including sharing information with partners and other organisations. Briefings and formal acceptance of security policies are required before access is granted to certain information systems and facilities. 3. There shall be adequate separation of functions for tasks that are susceptible to fraudulent or other unauthorised activity; Audit shall be consulted for advice on this. 4. Information users shall not attempt to access information to which they do not have authority. 5. Information users shall keep personal passwords confidential at all times. 6. Agreements and contracts with external business partners and suppliers shall include the requirement to adhere to this policy, where there is relevance to do so. 7. School equipment, facilities and information shall be used only for the School's business purposes, unless permission of line management has been obtained. School equipment, facilities and information must never be used for personal gain or profit.

	9. Non-School or personally owned equipment or storage devices shall not be connected to the School computer network or to any School-owned equipment, whether on the School's network or not, without permission from the ICT Technician. 10. All information about the security arrangements for School computer and network systems and structured manual filing systems is confidential to the School and shall not be released to people who are not authorised to receive that information.

3.3 The availability of information shall be protected.	1. Business continuity plans shall include all aspects of the School's infrastructure, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems, information on mobile devices and storage, communications including telephone services, staffing requirements, transport facilities, electricity supply, office accommodation and maps.
3.4 The integrity of information shall be maintained.	1. A named individual should have operational responsibility for the ICT systems and procedures (e.g. ICT Technician). Details of key staff are listed at ATTACHMENT 2 of this policy. 2. The accuracy and completeness of information, including structured manual filing systems, processing methods and computer software shall be protected from unauthorised modifications. Users shall not attempt unauthorised modifications. 3. Users shall use only the officially provided or approved facilities and systems to access School information. 4. Users shall not interfere with the configuration of any computing device without approval. 5. Update regularly all devices, which are subject to the threat of malicious software, with malicious software scanning software. 6. Update regularly all devices, which are subject to the threat of security vulnerabilities with appropriate security patches.

4. Monitoring of the Information Security Policy

The use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure that this policy is adhered to and to detect and investigate unauthorised use of information
- To maintain the effectiveness, integrity and security of the computer network
- To ensure that the law is not being contravened
- To protect the services provided by the School and Council to the public and protect the integrity and reputation of the School and Council.

All monitoring shall be:

- Fair and proportionate to the risks of harm to the School and Council's information and reputation
- Undertaken so as to intrude on users' privacy only as much as is necessary
- Carried out similarly regardless of whether the user is office based or working remotely
- Carried out subject to the requirements of legislation, e.g. Regulation of Investigatory Powers Act 2000. Access to any records of usage shall be stringently controlled.

5. Review of the Information Security Policy

This policy shall be reviewed at least annually. This policy and its associated policies, processes, procedures and guidelines shall be updated according to:-

- Internally generated changes e.g. changes in service strategy, organisation, locations and technology;
- Externally generated changes e.g. changes in legislation, security threats, security incidents, recommended best practice and audit reports;
- All changes shall be approved by the Head Teacher and School Governors and be made available to everyone to whom it applies.

6. Declaration

I accept that I have a responsibility to safeguard John Wycliffe Primary School information and equipment by abiding by the conditions of use defined in this Information Security Policy.

I understand that misuse of electronic and other communications may lead to consequences, which could be harmful to individuals, the Council, the School or other organisations. I understand that for certain types

of misuse, I may be open to criminal prosecution under the Obscene Publications Act, the Computer Misuse Act or the Data Protection Act.

I understand that in order to ensure that the Information Security Policy is properly followed, and to maintain the effectiveness, integrity and security of the network, the use of electronic communications will be monitored.

Signed: _____

Date: _____

7. Document Management

Document Disclaimer

This document is issued in confidence only for the purpose for which it is supplied.

Document Owner

John Wycliffe Primary School

Document Control

This document is controlled by the Head Teacher and Governors of the school. Any amendments should be discussed with them.

Other attachments relating to this policy:

Attachment 1: Glossary of Terms
Attachment 2: Key Contacts
Attachment 3: Reporting Information Security Breaches
Attachment 4: Passwords for Staff
Attachment 5: Other policy to support the Information Security Policy
Attachment 6: Document Retention and Disposal Policy

ATTACHMENT 1

Glossary of Terms

Accountability	The quality or state of being accountable, especially an obligation or willingness to accept responsibility or to account for one's actions. The ability to verifiably track actions to identifiable individuals.
Availability	Ensuring that authorised users have access to information and associated assets when required.
Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Information Security	The preservation of confidentiality, integrity, availability and accountability of information.
Information Security Risk Assessment	A structured method of analysing the risks to information. Risks consist of vulnerabilities (weaknesses) and threats. The selection of appropriate security controls is based on the likelihood of the risk occurring and the potential impact if the risk occurs.
Malicious Software	Any software written with the intention of doing damage, such as viruses, worms and spyware. The damage may be disclosure or loss of information, denial of access or making a computer unusable. Even if malicious software does no direct damage, covertly installed unauthorized software is still considered malicious.
PDA	Personal Digital Assistant – a small computing device used for diary management and e-mail.
Residual Risk	In general it is not possible or cost effective to remove all information risk - it might be technically impossible or not feasible on cost grounds. An understanding of the remaining "residual risk" allows it to be managed, for example by insurance. "Residual risk" is the level of risk that remains after controls have been introduced to manage the initial (inherent) risk.
Security Incidents and Weaknesses	A security incident (also called a security breach) is any event, which results in unauthorised access, loss, disclosure, modification or destruction of information whether accidental or deliberate. A security incident may not necessarily result in damage to information – it is still a breach of security. A security weakness is where there is potential for a security incident.
Structured Manual Filing Systems	Structured manual filing systems are called "relevant filing systems" in the Data Protection Act 1998, and are defined as "Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating

	automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

ATTACHMENT 2

Key Contacts

Owner and champion of the Information Security Policy

Job Title	Headteacher
Name	Mrs Vickie Njoroge
E-mail address	vnjoroge@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

System Administrator/ Network Manager:

Job Title	ICT Technician II
Name	Mrs Sally Butcher
E-mail address	sbutcher@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

SIMS System Administrator:

Job Title	Bursar
Name	Mrs Jill Mellar
E-mail address	schooloffice@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

Responsible Person for Information Security within the school

Job Title	Headteacher
Name	Mrs Vickie Njoroge
E-mail address	vnjoroge@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

Responsible Person for Data Protection/Freedom of Information Requests

Job Title	Headteacher
Name	Mrs Vickie Njoroge
E-mail address	vnjoroge@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

Primary person to report a security breach or weakness to:

Job Title	Headteacher
Name	Mrs Vickie Njoroge
E-mail address	vnjoroge@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

Deputy person to report a security breach or weakness to:

Job Title	ICT Technician II
Name	Mrs Sally Butcher
E-mail address	sbutcher@johnwycliffe.leics.sch.uk
Telephone no	01455 553135

ATTACHMENT 3

Reporting Information Security Breaches

You must report security incidents and weaknesses to the following people:

- Your Headteacher
- Your ICT Technician
- LEAMIS helpdesk Telephone: 0116 231 1280 E-mail: helpdesk@leamis.org.uk
- The Information Security Consultant at County Hall on (0116) 3057693
- Katie Robey, System Information Manager, Room G8, County Hall on (0116) 305 5783

You can make your report by phone, face to face, using the online form or by letter - whichever you prefer.

Examples of incidents:

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. memory sticks ;
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident ;
- Finding the doors and/or windows has been broken and forced entry gained to a secure room/building that contains service user records.

Breach of confidentiality/security

- Finding a computer printout with a header and a person's information on it at a location outside of School premises ;
- Finding any paper records about a service user/member of staff or business of the organisation in any location outside of the School premises ;
- Being able to view service user records in the back (or front) of an employee's car ;
- Discussing service user or staff personal information with someone else in an open area where the conversation can be overheard ;
- A fax being received by the incorrect recipient.

ATTACHMENT 4

Passwords for Staff

1. Never reveal your password to anyone else or ask others for their password.
2. 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.
3. There is a useful tool that will help identify how strong a password you are using – check your password out at http://www.microsoft.com/protect/yourself/password/checker.mspx
4. Users with administrative level access should ensure that they utilise a complex password – 6 random character/numbers in mixed case.
5. If you forget your password, please request that it be reset by the ICT Technician.
6. If you believe that a student or other staff may have discovered your password, then change it **immediately**.
7. Never use the feature 'Remember password'
8. Change passwords regularly.
9. Never leave your computer unattended while using any personal data
10. Never allow another person to login to any system with your login ID and password. Auditing measures in place could result in you being responsible for the actions of another person. This is particularly risky in a situation where you as an adult allow a child to access materials under your login.
11. Never write your password down and leave it out for others to find.

ATTACHMENT 5

Other policies to support the Information Security Policy

Available on EIS - http://eis.leics.gov.uk/schools

- The use of e-mail systems
- Secure Remote Access
- Biometric Technology
- Obsolete Equipment Disposal
- Selling School PCs and Laptops
- Encryption
- Impact Levels and labelling
- Audit Logging
- Case Recording
- Data Quality Strategy
- SIMS System Standards
- Information Governance Training Booklet
- Fair Processing Notice's
- Data Protection Act 1998
- Freedom of Information Act 2000

Corporate Information Security

- E-communications Usage Policy
- Information Security Policy
- Information Security Policy leaflet
- Information Security Risk Assessment Report Template

E-Safety Website
http://eis.leics.gov.uk/esafety

LCC Whistleblowing Policy
http://www.leics.gov.uk/whistleblowing_for_employee

External Links

Data handling guidance for schools
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

Details about information sharing on the DCSF website
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

ATTACHMENT 6

Document Retention and Disposal Policy

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule. The schedule should list the types of documents the school holds, how long they should be kept for and how they should be destroyed. Members of staff are encouraged to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems. The retention schedule refers to all information, regardless of the media in which it is stored.

Benefits of a retention schedule

There are a number of benefits which arise from the use of a complete retention schedule:

a. Managing records against the retention schedule is deemed to be "normal processing" under the Data Protection Act 1998 and the Freedom of Information Act 2000.

b. Members of staff can be confident about destroying information at the appropriate time.

c. Information which is subject to Freedom of Information and Data Protection legislation will be available when required.

d. The school is not maintaining and storing information unnecessarily.

The school adapted the LCC model policy and it was approved and adopted by the Governing Body in May 2008.

The password protected inventory is maintained by the Bursar and ICT Technician within the school SIMS system. The following information is included in each record.

Equipment
Description
Assigned to
Manufacturer
Serial No (where applicable)
Location
Date purchased
Date of disposal
Audit date

ATTACHMENT 7

Memory Stick/External Portable Hard Drive Policy

Despite their small size, USB memory sticks and portable hard drives have a very large capacity and therefore pose a considerable security risk if they are lost, stolen or abused.

All memory sticks and external hard drives owned by school for storing sensitive information are password protected and encrypted; the school recommends that memory sticks are not used apart from in those circumstances documented below or where a strong business case can be applied. This should be approved and not made in isolation.

1. A memory stick/hard drive can be used to transport information that is not personal or sensitive from the users main LCC PC/Laptop to another PC/Laptop that has up to date anti-virus software installed upon it for example for a presentation.

2. A memory stick/hard drive can be used for transporting sensitive information where there is a legitimate business reason to do so. For example, where no alternative provision such as a laptop can be used.

In order to mitigate the risks associated with this the school has also adopted the following controls and monitoring processes:-

1. All staff that requires such equipment will only be assigned an encrypted USB memory stick or portable hard drive

2. Prepare guidance notes to outline staff acceptable use of the memory stick or portable hard drive.

3. Staff will be required to produce their memory stick or portable hard drive if requested on demand to ensure it hasn't been misplaced.

4. Regularly advertise the incident reporting process so that any loss or breach can be reported confidentially if needed.

5. Users should investigate alternative methods of safe transportation before the memory is used.

Appendix E

E-Safety Incident Log

Organisation address	Moorbarns Lane, Lutterworth, Leicestershire, LE17 4QJ.		
Organisation contact details	Tel: 01455 553135 Email: schooloffice@johnwycliffe.leics.sch.uk		
E-safety lead	Sally Butcher		
E-safety lead contact details	Tel: 01455 553135 Email: sbutcher@johnwycliffe.leics.sch.uk		
Details of incident			
Date		Time	
Where did the incident occur			
Name and contact details of the person reporting the incident			
Who was involved in the incident	□ child/young person □ staff member □ other (please specify) _____		
Names and contact details of those involved			
Type of incident	□ bullying or harassment □ online bullying or harassment (cyberbullying) □ sexting (self-taken indecent imagery) □ deliberately bypassing security or access □ hacking or virus propagation □ racist, sexist, homophobic religious hate material □ terrorist material □ other (please specify)_____		

Description of incident	
Nature of incident	□ deliberate access □ accidental access
Did the incident involve material being	□ created □ viewed □ printed □ shown to other □ transmitted to others □ distributed
Could this incident be considered as	□ harassment □ grooming □ cyberbullying □ sexting (self-taken indecent imagery) □ breach of AUP □ other (please specify) _____
Action taken	□ **staff** □ incident reported to headteacher/senior manager □ advice sought from children's social care □ incident reported to police □ incident reported to Internet Watch Foundation □ incident reported to IT □ disciplinary action to be taken □ e-safety policy to be reviewed/amended □ **child/young person** □ incident reported to staff member (name) _____ □ incident reported to social networking site □ incident reported to IT □ child's parents informed □ disciplinary action taken □ child/young person debriefed □ e-safety policy to be reviewed/amended

Outcome of incident/investigation

Children's social care	
Police/CEOP	
Organisation	
Individual (staff member/child)	
Other (HR/legal etc)	

Learning from the case

Key learning point 1	
Key learning point 2	
Key learning point 3	
Key learning point 4	

Recommendations and timescales to implement

Recommendation 1		Timescale to be implemented	
Recommendation 2		Timescale to be implemented	
Recommendation 3		Timescale to be implemented	
Recommendation 4		Timescale to be implemented	

Validation

Signed		Print Name Date	
Signed		Print Name Date	
Signed		Print Name Date	
Signed		Print Name Date	

Appendix F

List of Authorised Persons

Name	Role
Vickie Njoroge	Headteacher
Sally Butcher	ICT Technician II
Jo Hodder	Deputy Head/Designated Senior Person
Deb Horton	Designated Senior Person