Wigston Academy

DIGITAL TECHNOLOGIES, TELEPHONE AND E-SAFETY POLICY

Original Policy Date:

Next Review Date:

Date approved by Directors:

Signed by Chair of Directors:

Contents

1. Introduction

Wigston Academy recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

To facilitate this we have taken a whole school approach to E-safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

Wigston Academy holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using digital technologies. We recognise that ICT can allow disabled pupils increased access to the curriculum and other areas related to learning.

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

The nominated persons for the implementation of the School's e-Safety policy are the Headteachers and Designated Safeguarding Leads.

2. Scope of Policy

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.

Wigston Academy will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- 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 the Internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- a reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Wigston Academy 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 Service Network (emPSN) who provide the network, services and facilities that support the communication requirements of the East Midlands learning community. As part of our commitment to partnership working, we fully support and will continue to work with emPSN to ensure that pupil and staff usage of the Internet and digital technologies is safe.

3.1.2 Wigston Academy will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that sees the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

4. Policies and Procedures

We understand that effective polices and procedures are the backbone to developing a whole-school approach to E-safety. Policies are aimed at providing a balance between exploring the educational potential of new technologies safeguarding pupils.

4.1 Use of Internet facilities, mobile and digital technologies

Wigston Academy will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 Wigston Academy expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below: These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

- 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 to peers or colleagues e.g. abusive 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 also permission is 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
- Software piracy
- Other criminal activity

4.1.5 In addition, users may not:

- Use the emPSN or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves emPSN in any way;
- Visit sites that might be defamatory or incur liability on the part of emPSN or adversely impact on the image of emPSN;

- 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;
- 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, representing personal opinions or 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 mobile or digital technologies 3G or mobile Internet services 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 (provider of Internet connectivity and associated services to schools) and/or emPSN become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will 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 will 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**.

4.2.2 The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB 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 Safeguarding Lead within the School will follow the established safeguarding policy and procedures and refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

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

5. Education and Training

5.1 Wigston Academy recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

5.2 As part of achieving this, we want to create within 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 the Internet and other digital technologies safely.

5.3 To this end, the School will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

6. Standards and Inspection

Wigston Academy recognises the need to have regular inspections of 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 the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. The School recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, we 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.

.1.3 Another aspect of monitoring, which our school will employ, is 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 policies 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 Wigston Academy has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

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

- *Child / Young Person*
    - The child/young person will be disciplined according to the behaviour policies of the school, which could ultimately include the use of Internet and email being withdrawn.
    - 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 instance, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to the IT Manager or a Designated Safeguarding Lead so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents and Carers

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

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

8. Appendices of the E-safety Policy

8.1 There are multiple aspects of the school’s E-safety policy, which include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention. The various policy documents relating to these aspects of the school’s E-safety policy can be obtained from the IT Manager for scrutiny, if required.

APPENDIX A

Model Acceptable Use Policy (Pupils)

Why have an Acceptable Use Policy?

An Acceptable Use Policy is about ensuring that you, as a pupil at Wigston Academy 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 environments and websites.

An 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 proxy sites as well as anonymous proxy sites, because they put the school network at risk.
Help us, to help you, keep safe.

Wigston Academy recognises the importance of ICT in education and the needs of students to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. To allow for this Wigston Academy requires all students to sign a copy of the Acceptable Usage Policy **before** they receive their username and password.

Listed below are the terms of this agreement. All students at Wigston Academy are expected to use the ICT facilities in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Management Policy of the School.

Please read this document carefully and sign and date it to indicate your acceptance of the Policy. Access to the School's ICT facilities will only take place once this document has been signed by **the pupil**.

1. Equipment

1.1 Vandalism

Vandalism is defined as **any action** that harms or damages any equipment or data that is part of the School's ICT facilities. Such vandalism is covered by the Computer Misuse Act 1990 (see Glossary). This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware.
- Change or remove of software
- Unauthorised configuration changes
- Create or upload computer viruses
- Deliberate deletion of files.

Such actions reduce the availability and reliability of computer equipment; and puts at risk other users' data. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every students' ability to use the ICT facilities. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities the School has.

1.2 Use of Removable Storage Media

Wigston Academy accepts the fact that you may wish to transfer school work done at home to school using a flash memory device. However, Wigston Academy cannot guarantee that your work will be able to be transferred properly using these. These must be scanned for viruses first by a member of the IT Team.

1.3 Printers and Consumables

Printers are provided across the Wigston Academy for use by staff to print students work. Please use the printers sparingly and for educational purposes only. Take the time to check the layout and proof read your work using the 'Print Preview' facility before printing.

If you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the School which includes the following:

- A warning
- Email and/or Internet facilities removed
- Letter home to parents
- Loss of access to the print facilities available within the School
- Report to the School Governors
- Report to appropriate external agencies like the Police

1.4 Data Security and Retention

All data stored on the Wigston Academy network is backed up daily. If you should accidentally delete a files or files in your folder or shared area, please inform a member of the IT Team immediately so that it can be recovered.

2. Internet and Email

2.1 Content Filtering

Wigston Academy provides layers of internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, **you must report it to a member of staff *immediately.***

The use of Internet and email is a privilege and inappropriate use will result in that privilege being withdrawn.

2.2 Acceptable use of the Internet

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

- Only access suitable material – the Internet is not be used to download, send, print, display or transmit material that would cause offence or break the law.
- Do not access Internet Chat sites. Remember you could be placing yourself at risk.
- Never give or enter your personal information on a website, especially your home address, your mobile number or passwords.
- Do not access online gaming sites. Remember that your use of the Internet is for educational purposes only.

- Do not download or install software from the Internet, as it is considered to be vandalism of the School's ICT facilities.
- Do not use the Internet to order goods or services from on-line, e-commerce or auction sites.
- Do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.
- Do not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

2.3 Email

You are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal or likely to cause offence should not take place.

Remember when sending an email to:

- **Be Polite** - never send or encourage others to send abusive messages.
- **Use appropriate language** - remember that you are a representative of the School on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
- **Do not reveal any personal information about yourself or anyone else**, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.
- **Consider the file size of an attachment,** files exceeding 1MByte in size are generally considered to be excessively large and you 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 that may cause loss of data or damage to the School network.

3.0 Privacy and Data Protection

3.1 Passwords

- **Never** share your password with 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.
- If you forget your password, inform the teacher immediately.
- If you believe that someone else may have discovered your password, then **change it immediately** and inform a member of staff.

3.2 Security

- **Never** attempt to access files or programs to which you have not been granted access to. 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 a member of staff

- If you are identified as a security risk to the School's ICT facilities you will be denied access to the systems and be subject to disciplinary action.

3.3 Storage and Safe Transfer of Personal Data

- Wigston Academy holds information on all pupils and in doing so, we must follow the requirements or the Data Protection Act 1998 (see Glossary). This means that data held about pupils can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Wigston Academy will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured.

4.0 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 Wigston Academy ICT system is at your own risk. Wigston Academy specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

5.0 Mobile Technologies

For reasons of safety and security pupils should not use their mobile phone out of school or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 3G 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 pupils 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, videos etc report it **immediately to a member of staff** within the school**.**

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 a fellow pupil's password and use it.

    - Unauthorised access to deliberately commit an unlawful act e.g. if you guess and fellow pupil'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, including teaching staff, support staff, volunteers and governors.

  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
    - Secure
    - Not transferred to other countries without adequate provision.

- 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.

APPENDIX B

Authorised Acceptable Use Policy (Staff, Governors and Volunteers)

Why have an Authorised Acceptable Use Policy?

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

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

Wigston Academy strongly believes in the educational value of ICT and recognises its potential to enable staff and volunteers in delivering and supporting the curriculum. Wigston Academy 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 is that both staff and volunteers will play an active role in implementing school and departmental Internet safety polices through effective classroom practice.

Wigston Academy 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, Wigston Academy 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. This policy is consistent within the "Guidance for Safer Working Practice for those working in educations – October 2015" document which is issued to all members of staff at Wigston Academy. 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 Wigston Academy 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). Wigston Academy assumes responsibility of maintenance of all hardware and software. mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware
- Deliberate deletion of files.
- The uploading of 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 and ipads

Laptop computers and ipads are issued to all teaching staff as required. Laptops and ipads remain the property of Wigston Academy at all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Wigston Academy at all times and must be returned to Wigston Academy at the end of the agreement or contractual period.
- Maintenance of the equipment is the responsibility of the Wigston Academy. All maintenance issues must be referred to the ICT Technical Department, through the usual channels.
- All installed software MUST be covered by a valid license agreement held by Wigston Academy.
- All software installation MUST be carried out by the ICT Technical Department 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.
- For laptops antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. *This should be done at least monthly*.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up to a memory stick or to the 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.
- Wigston Academy 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 Wigston Academy 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 memory devices to transfer files between home and school, Wigston Academy 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. Wigston Academy cannot guarantee the correct operation of flash memory devices on the system, although every effort is made to ensure that this facility is available. All removable media should be scanned for viruses before use.

1.4 Printers and Consumables

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

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

1.5 Data Security and Retention

All data stored on the Wigston Academy network is backed up daily and backups are stored for up to at least two weeks. If you should accidentally delete a files or files in your folder or shared area, please inform the IT Team *immediately* so that it can be recovered.

2. Internet and Email

2.1 Content Filtering

Wigston Academy 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 IT Team 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 IT Team assumes responsibility for all software upgrades and installations.

2.3 Appropriate use of email by staff

Staff are provided with an email address by the 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 10MByte 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.

3.0 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 via the IT Team.
- If you believe that a student or other staff may have discovered your password, then change it ***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 IT Team.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with Leicestershire County Council Disciplinary Procedures for Local Government Services Employees.

4.0 Management and Information Systems [if applicable]

Access to MIS software is available only from designated locations and only to those staff who require it. Access is subject to agreement with Mrs C Reeds. Usage of MIS software is subject to the following guidelines:

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

5.0 Mobile Technologies

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.

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 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**.

6.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to the IT Team.

6.1 Software Installation [if applicable]

The IT Team 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 period of notice is required for packaging and installation of new software.
- Software cannot be installed on the *School's* network without a valid license agreement. This must be supplied with the software package.
- Please check the licensing terms of the software package carefully to ensure that it is suitable for use on the School network. If you are unsure, please ask the IT Team for assistance or contact the software supplier. A relevant and valid license agreement document will be required before any software packages can be installed.
- All software installation media and license agreements are held centrally within the Wigston Academy 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 Wigston Academy network, please check its suitability, compatibility and licensing terms. Purchase orders for new software will normally be authorised only with the agreement of the IT Team.

6.2 Service Availability [if applicable]

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 Wigston Academy ICT system is at your own risk. Wigston Academy specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

<u>Glossary</u>

- 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
- Secure
- Not transferred to other countries without adequate protection

- RIPA – Regulation of Investigatory Powers Act 2002

  If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

  - the interception of communications
  - the acquisition and disclosure of data relating to communications
  - the carrying out of surveillance
  - the use of covert human intelligence sources
  - access to electronic data protected by encryption or passwords

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

REQUIRED SIGNATURE

MEMBER OF STAFF/VOLUNTEER

I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to the *[specifed member of staff or department]*. 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 C

INTERNET ACCESS AND HARDWARE

The use of workstations in school offices is to exclusively for administration purposes.

The installation of the internet to the school was completed on the understanding that it would be used for educational and administration use only and is monitored by the ICT Technical Department on this basis.

Office staff would also be grateful if you could use office workstations to a minimum as they are needed to do the work of the office during school hours.

LAPTOPS

Upon receipt of a school laptop teachers will need to:

- Sign a letter accepting responsibility for the laptop.
- Ensure laptop is entered onto school inventory via the IT Manager.
- Insurance company needs to be notified of serial number, make and model via the Chief Operating Officer.

Laptops should:

- Be protected against the possibility of virus infection. Anti virus software is pre installed but should be regularly updated by the user.
- Be used in accordance with the Data Protection Act 1998: The Act requires, amongst other things, that all personal data should be protected by appropriate security safeguards against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage. This particularly applies to pupil data held on the laptop and especially so if taken off site.
- Be used in accordance with the Copyright, Design and Patents Act 1988: All software must be used only in accordance with the terms of the licence. Generally, the making of copies is forbidden and is a criminal offence.
- Be used in accordance with the Computer Misuse Act 1989: The act identifies three main offences concerning unauthorised access to system, software or data. The punishment depends upon whether the intent of the hacker was merely to gain access, to commit further offences after gaining access or to make a modification to 'computer material' e.g. to inject a virus.
- Be used in accordance with school, LA and GTC policies on the inappropriate use of computers.

- Laptops remain the property of the school and as such must be passed to A Marshall when any teacher leaves the school or is on extended leave (illness, maternity, etc) so that they can be used by other staff covering the absence. The use of school laptops for personal use is not allowed.

DAMAGE TO ICT EQUIPMENT

To all staff

Please be aware that any damage caused to school ICT equipment will be charged as follows:

1. Laptops – either to the member of staff loaning the equipment from school or the school if damage relates to ‘wear and tear’.

2. In school ICT equipment e.g. whiteboards, including leads, workstations and accessories – either to the department or the school if damage relates to ‘wear and tear’.

APPENDIX D

THE USE OF ICT TO IMPROVE EFFICIENCY

Information now shared or managed in school via ICT as a matter of routine.

1. SEN
   - Start of the year information e.g. reading/spelling ages.
   - IEPs.

2. ADMINISTRATION
   - Staff Handbook (excepting academic administration to be issued via email).
   - Calendar.
   - Notes of meetings/agendas.
   - Notice/messages/request for information via email/Pastoral Team memos.
   - Registers.
   - Timetables e.g. Learning Reviews.
   - Progress and attainment data.
   - Data for reports.

3. CURRICULUM
   - Plans via VLE.
   - Trackers.

4. PARENTS
   - Aspire Newsletters and announcements via email.
   - Text messages for absences etc.
   - Parent pay for payments.
   - Reports and attendance data available online.

5. WEBSITE
   - Letters to parents.
   - Trips and Visits information.
   - Print Shop.
   - Aspire.

APPENDIX E

NOTE TO ALL STAFF (TEACHING AND SUPPORT STAFF)

SOCIAL NETWORKING SITES

Advice:

It is not acceptable in relation to e-safety or school ethos to engage on-line with ex pupils who are still in the education system (or under the age of 18) or accept them as ‘friends’ on social networking sites.

I assume that no-one is entering into conversations or accepting as ‘friends’ any current pupils at the school. This is not allowed under Safeguarding Regulations.

Alex Green
January 2016