BARWELL ACADEMY
CHURCH OF ENGLAND
BELIEVE ACHIEVE SUCCEED – LEARNING THAT LASTS A LIFE TIME

BARWELL CHURCH of ENGLAND ACADEMY

ONLINE SAFETY POLICY

1. Introduction

1.1 *Barwell CE 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.

1.2 As part of our commitment to learning and achievement we 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.
- Develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material.
- Develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- Use existing, as well as up and coming, technologies safely.
- Enhance the children's learning experience.
- Engage in independent and collaborative learning using the internet and other digital technologies.

To enable this to happen, we have taken a whole school approach to Online Safety as promoted by British Education Communication Technology Agency (BECTA) and CeOP materials, which include 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. These have been adapted to reflect the school's own decisions on balancing educational benefit with potential risks. This Online Safety policy will be used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

1.3 Barwell CE Academy, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.

Barwell CE Academy is committed to ensuring that **all** its pupils will be able to use existing, as well as up–and-coming 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.

1.4 The nominated senior person for the implementation of the School's Online Safety policy is the Headteacher, Miss Victoria Newman.

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 Barwell CE Academy 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 Online Safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated by staff, governors, parents and children;
- 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 mobile technologies;
- education that is aimed at ensuring safe use of Internet and mobile technologies;
- a reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Barwell CE 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 Broadband Community (Openhive) 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 Openhive to ensure that pupil and staff usage of the Internet and digital technologies is safe.

3.1.2 Barwell CE 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 or mobile technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

4. Policies and Procedures

We at Barwell CE Academy understand that effective polices and procedures are the backbone to developing a whole-school approach to Online Safety. The policies that exist within Barwell CE Academy 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

4.1.1 Barwell CE 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 Barwell CE Academy 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 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
    - Grooming
    - Acts of Cyber-bullying
    - 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.

[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.

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 <u>In addition, users may not:</u>

- Use the Openhive or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves Openhive or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of Openhive or member Local Authorities or adversely impact on the image of Openhive;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Openhive, or to Openhive 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 Openhive
- Undertake activities with any of the following characteristics:

- wasting staff effort or networked resources, including time on end systems accessible via the Openhive 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 Openhive 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 Openhive has requested that use cease because it is causing disruption to the correct functioning of Openhive;
- other misuse of the Openhive 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.

Staff are only permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils with the express permission of the Headteacher. Images can be taken only of those children with parental consent and must be transferred immediately to a school device or network and deleted from the staff device.

4.1.6 Where Synetrix (provider of Internet connectivity and associated services to schools) and/or Openhive 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.

4.1.7 **The School Website**

Details on the school Web site include the school contact address, e-mail and telephone number. Staff or pupils' personal information will not be published. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

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 such as Cyberbullying 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 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[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

5.1 Barwell CE 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 Barwell CE Academy 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, Barwell CE Academy will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Ensure that children of all classes are aware of e-safety issues and take part in Insafe's 'Safer Internet Day where children explore issues of Online Safety
- 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.

Whole-School Responsibilities for Internet Safety

Headteacher

- Responsible for Online Safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader as the e-safety co-ordinator.

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

- Ensure that the e-safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that the Governing Body is informed of Online Safety issues and policies.
- Ensure that appropriate funding is allocated to support Online Safety activities throughout the school.

E-safety co-ordinator

- Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).
- Establish and maintain a school-wide Online Safety programme.
- Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
- Establish and maintain a staff professional development programme relating to Online Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation.

Governing Body

- Online Safety will be reviewed as part of the regular review of child protection and health and safety policies.
- Support the Headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for Online Safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety coordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Teaching and Support Staff

- Contribute to the development of Online Safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Embed Online Safety education in curriculum delivery.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within & outside school.
- Take responsibility for their professional development in this area.

Wider School Community

As a school we aim to encourage:

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet or other technologies present within school.
- Contribute to the development of Online Safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.

- Know when and how to escalate Online Safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

6. Standards and Inspection

Barwell CE 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. Barwell CE Academy recognises that in order to develop an effective whole school Online 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, Barwell CE Academy 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.

6.1.3 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 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 Barwell CE 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 policy 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 Headteacher, Miss Victoria Newman and Openhive so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents and Carers

7.1 Barwell CE 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.

We at Barwell CE 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.

As a school we aim to encourage:

- Contribute to the development of Online Safety policies.
- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school internet and/or Learning Platform.
- Discuss e-safety issues with their children, support the school in its Online Safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

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 Headteacher, Victoria Newman, for scrutiny, if required.

ICT Acceptable Use Policy (pupils)
Barwell CE Academy

Barwell CE Academy 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 Barwell CE Academy 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 Barwell CE Academy 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 as monitors, base units, printers, keyboards, mice or other hardware such as iPads
- Deliberate 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 Barwell CE Academy for use by pupils. It is important that children learn to press the print key only once and then wait and be patient.

2. Internet and Email...

2.1 Content Filtering and use of the Internet

Barwell CE Academy provides four 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 filtering services provided by Openhive which seeks to provide internet use that is safe and for educational purposes only.

2.3 Email

As part of your child's work in Computing 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. This allows access only to children's search engines such as "SafeSearch for kids"
- Children are not allowed access to enter 'chat rooms' at any time
- Children in all year groups are taught about safe Internet use by their teachers

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

Barwell CE Academy 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:

- The 'Abacus' Learning Platform is provided for use of Barwell CE Academy 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 Learning Platform remote access service is provided by Abacus and Barwell CE Academy can make no guarantees as to service availability or quality.

4.0 Privacy and Data Protection

4.1 Passwords

Children will be given simple and an easy to remember password which they will learn to use

5.0 Mobile technologies

For reasons of safety and security your child should not use his/her mobile phone or any other mobile or fixed technology outside of school in a way that is likely to damage the reputation of the school or risk the welfare of any 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.

6.0 Service

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school cannot be held 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 errors or omissions. Use of any information obtained via the Barwell CE Academy ICT system is at your own risk. Barwell CE Academy specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

- -

Required Signature

PARENTS / CARERS

I have read this 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 Barwell CE Academy

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 at Barwell CE 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 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.

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

Barwell CE 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, Barwell CE 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. 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 by either volunteers or governors, the school will seek advice and support from the Local Authority in order to manage the situation in a fashion that safeguards the school's population and reputation.

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 Barwell CE 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). The School assumes responsibility for 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 of 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

Laptop computers are issued to all teaching staff and to support staff as required. iPads are issued to assigned staff. Laptops and iPads remain the property of Barwell CE Academy all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Barwell CE Academy at all times and must be returned to the School at the end of staff's employment at the school, or when an updated item is issued.
- Laptops issued to staff are supplied with encryption software fitted which must not be removed. This is essential to protect data in the event of an attempt to access files by unauthorised persons.
- Laptops and iPads are issued to staff to support them in their assigned school roles. Any occasional personal use of school hardware or software is also strictly subject to these AUP guidelines.
- Maintenance of the equipment is the responsibility of the 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 Barwell CE Academy.
- All software installation MUST be carried out by the ICT technician in accordance with the relevant license agreements.

- No school software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual technical support channels.

- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the internet to ensure virus definitions are kept up to date.

- 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 CD-RW disk, a memory stick, a supplied encrypted external hard drives or to the Barwell CE Academy 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.

- Barwell CE 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 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

Mobile storage media (flash drives and external hard drives) issued to staff are supplied with encryption software fitted which must not be removed. This is essential to protect data in the event of an attempt to access files by unauthorised persons.
All files containing personal data of staff or pupils stored in transportable form within or outside of school must be held on devices which are encrypted. Barwell CE Academy cannot guarantee the correct operation of flash memory devices or external hard drives 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 through staff codes that are issued at the beginning of the academic year.

- 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 Barwell CE Junior network is backed up daily and backups are stored for up to at least two weeks[4]. If you should accidentally delete a file or files in your folder or shared area, please inform the ICT Technician immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 4 weeks previously.

2. Internet and Email

2.1 Content Filtering

Barwell CE Junior 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 in school. These represent a significant security threat to the School's network.

- The use of online gaming sites is prohibited at all times on any hardware owned by the School. These consume valuable network resources that may adversely affect the performance of the system. This ban applies to school hardware used outside of school.

- 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.

[4] The duration of data being stored on the school network is an issue that the school ICT Co-ordinator/Network Managers will need to decide upon in conjunction with the Headteacher and other members of the school leadership team.

- Do not attempt to download or install software on to networked computers 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 Barwell CE Academy. 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 5MByte in size are generally considered to be excessively large and staff should consider using other methods to transfer such files.

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

3.0 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 Barwell CE Academy staff and students only. Access by any other party is strictly prohibited.

- By using Web-Email, you signify that you are an employee of Barwell CE Academy 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. Barwell CE Junior accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

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

4.0 Privacy and Data Protection

4.1 Passwords

- Never 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 ICT Technician.
- If you believe that a student or other staff may have discovered your password, then change it ***immediately***.

4.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.

- 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 subject to disciplinary action in accordance with Leicestershire County Council Disciplinary Procedures for Local Government Services Employees.

5.0 Management and Information Systems

Access to MIS software is available only from designated locations and only to those staff who require it. Access is subject to agreement with the school leadership team. 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, please 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 Barwell CE Junior it is understood that the Headteacher and Senior Leadership team have a clear duty of care to protect the access to confidential data.

- Where staff are working at home and connect remotely to the school’s MIS system then all of the above considerations also apply. Staff must ensure that their home Internet connection is secure from outside access particularly if a wireless network is used. Additionally staff should take due care of any material which they print at home.

6.0 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**.

Staff are only permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils with the express permission of the Headteacher. Images can be taken only of those children with parental consent and must be transferred immediately to a school device or network and deleted from the staff device.

7.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to the ICT Technician

Barwell CE Junior will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

7.1 Software Installation

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

- Notice is required.

- 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 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 Barwell CE 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 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 Head teacher.

7.2 Service Availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the School will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information

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

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 Head teacher. 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

_____