BARWELL ACADEMY

CHURCH OF ENGLAND

BELIEVE ACHIEVE SUCCEED – LEARNING THAT LASTS A LIFE TIME

The Great Barwell Adventure

Online Safety Policy

(including Acceptable Use)

Love thy neighbour in a flourishing school community. A community with Jesus' protective love at heart, celebrating diversity with the highest expectations for all, both academically and behaviourally. A community that puts physical and mental wellness at its heart. A loving, knowledgeable community building a rich, challenging curriculum for all.

Approved by:		Date:
Last reviewed on:		
Next review due by:		

Contents

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Support the school in teaching pupils safe and effective internet and ICT use
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy covers all users of our school's ICT facilities, remote learning platforms and services, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our school Disciplinary Policy, Staff Handbook and Behaviour Policy.

2. Relevant legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

In summary, this policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools
- Protecting children from radicalisation: the prevent duty

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications, online platforms or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities or the online platform and services, including governors, staff, parents, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety incidents as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is Alex Cole.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The Deputy DSL (Computing Lead) in conjunction with the Headteacher, takes responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with Leamis (IT support service), computing lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Senior Leadership Team and/or governing body. This list is not intended to be exhaustive.

3.4 The ICT Support Service

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 3 and 5)
- Working with the Deputy DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and (appendix 4)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- National Online Safety: https://nationalonlinesafety.com/login
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly, including protecting their online identity and privacy
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised with DSLs.

Concerns or queries about this policy can be raised with the headteacher or governing body.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (see the school Anti-Bullying Policy)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness or bystander rather than the victim.

The school will actively discuss cyber-bullying with pupils explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies and other key events.

Teaching staff are also encouraged to find opportunities to use other aspects of the curriculum to cover cyber-bullying. This includes throughout our Journey to Wellness (including personal, social, health, citizenship) and other subjects where appropriate

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. Parents also have access to National Online Safety (an online platform designed to support parents in their understanding of the latest technology).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Lead DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services, if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or

files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. Unacceptable use

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 2, 3 and 4). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 2, 3, 4 and 5.

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 8.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data

- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

8.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion. In this case, staff are instructed to discuss the issue with the Headteacher/Chair of Governors.

8.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Disciplinary Policy, Staff Handbook, Behaviour Policy.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

9. Staff (including governors, volunteers, and contractors)

9.1 Access to school ICT facilities and materials

The ICT manager/support service manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Users will be provided with unique log-in/account information that they must use when first accessing the school's ICT facilities. This must then be changed to a personal password following the advice of the school's password policy.

Users who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the support services.

9.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials directly using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract and must remain professional at all times

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be password protected so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If you are in receipt of an email containing personal data, you should also advise the sender to inform their Data Protection Officer of the breach.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in appendix 6.

The school can record in-coming and out-going phone conversations and virtual meetings.

If you record calls or meetings, callers or attendees **must** be made aware that the conversation/meeting is being recorded and the reasons for doing so. Staff who would like to record a phone conversation or virtual meetings should speak to DSLs before making the call.

All non-standard recordings of phone conversations or virtual meetings must be pre-approved, and consent obtained from all parties involved.

9.2 Using ICT facilities for personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not constitute 'unacceptable use', as defined in section 8.
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purpose
- Is proportionate, professional and appropriate

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Bring Your Own Device Policy (appendix 6) Camera facilities on a personal device must not be used to take photographs or videos.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (appendix 1) and use of email (see section 9.1.1) to protect themselves online and avoid compromising their professional integrity.

All personal devices must be password protected to the tune of a six-digit pin code or through biometric access.

9.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (appendix 1).

9.3 Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT support service.

9.4 Remote access

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take the same precautions as being on-site.

We allow staff to access the school's ICT facilities and materials remotely through various platforms including Microsoft Office 365, ParentPay and CPOMS – this list is not exhaustive.

The different platforms are managed by the appropriate bodies with the support of the ICT support services. Where appropriate, in an effort to protect sensitive and personal data (for example: Office 365 and CPOMS) staff have multi-factor authentication log in when signing in increasing the security of their accounts. When a password reset is required, the computing lead is informed and a temporary password is applied and sent to the relevant member of staff.

In agreement with their laptop loan agreement, Bitlocker encryption is also installed on staff laptops, increasing the security of our remote access. Staff are required to input an encryption code at each turn on.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

9.5 School social media accounts

The school has five official Twitter pages (@BarwellAcademy, @Year3Barwell, @Year4Barwell, @Year5Barwell, @Year6Barwell and @TheEarlyBirdsN1) managed by the headteacher, class teachers and Wrap Around Care Leader respectively. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

9.6 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

10. Pupils

Access to ICT facilities and equipment on the school site are available to pupils only under the supervision of staff.

- In terms of remote learning, pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using: https://www.microsoft.com/en-gb/microsoft-teams/log-in. They are also able to download the Microsoft Teams app in order to access their online content.
- If children forget their password or are locked out of their account, they are required to inform a member of staff who will then, in turn, alert the computing lead who will send an alternative password to the office. The office will then notify parents of the new password.

10.2 Use of personal devices

Pupils can only bring mobile devices into school after acquiring permission from their parent/carer. They must be handed in to the class teacher in the morning to be locked away securely and returned at the end of the day. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10.3 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

11. Parents

11.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

11.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 4.

12. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

12.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts. To protect our accounts from cybercrime, staff must choose a password consisting of three random words with at least one number and one special character for additional and enhanced security.

Staff will be required to change their passwords every 90 days. This will automatically be applied through Microsoft 365 admin and staff will be reminded 14 days before their password is due to expire.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

12.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

12.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's Data Protection Policy.

12.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by ICT support services.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Senior Leadership Team or ICT support services immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

12.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by this policy.

13. Internet access

The school wireless internet connection is secured.

Barwell CE Academy provides several 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 Netsweeper which seeks to provide internet use that is safe for all pupils.

When pupils log on to the network, filtering would be at a different level to the adult filtering which has been applied to each adult logon throughout the network. Guest access to wifi has also been established as 'Barwell Guest' which also ensures an appropriate level of filtering for vistors to our school.

Although we have a high level of filtering in our school, please be aware that filters are not foolproof. Inappropraite sites that the filter has not identified should be reported immediately to the ICT Managers Providers. In a similar fashion, if there are appropriate sites that have been filtered, please contact the ICT Managers.

13.1 Pupils

Our school wifi is unavailable for pupil use unless using as part of the school's ICT facilities and only when supervised by adults. Pupils are not permitted to request access for personal devices at any time.

13.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

14. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

15. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The lead DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

16. Monitoring and review

The headteacher monitors the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years. At every review, the policy will be shared with the governing body..

The governing body is responsible for approving this policy.

17. Related policies

This policy should be read alongside the school's policies on:

- Anti-Bullying Policy
- Staff discipline procedures
- Data protection
- Child Protection and Safeguarding policy
- Behaviour Policy
- Data Protection policy and privacy notices
- Complaints procedure
- Staff Handbook

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

Guidance for school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Avoid using social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Remember… As part of your professional standing in school, any action which brings the school into disrepute may result in disciplinary action or dismissal.

Check your privacy settings

- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify Senior Leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the Senior Leadership Team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors

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

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school • As part of your professional standing in school, any action on social media which brings the school into disrepute may result in disciplinary action or dismissal.	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Acceptable use agreement for pupils

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

Acceptable use of the school's in-school ICT facilities and internet: agreement for pupils	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

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

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Twitter page • Email/text groups for parents (for school announcements and information) • Our virtual learning platform – Microsoft Teams Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure	
Signed:	**Date:**

Appendix 5: Acceptable use agreement for Remote Learning for pupils.

BARWELL ACADEMY

CHURCH OF ENGLAND

BELIEVE ACHIEVE SUCCEED – LEARNING THAT LASTS A LIFE TIME

The Great Barwell Adventure

Online Remote Learning Responsible User Agreement

Remote learning requires access to any online platforms and services maintained by Barwell Academy and will require you to communicate with teachers and fellow pupils in a mature and considerate manner. This user agreement is to be used in conjunction with the general Acceptable Use Policy. By logging in to the School's systems you agree to the terms of this Policy.

The below rules will help to ensure that all members of our Barwell Academy community are able to be supported academically and pastorally when working remotely.

1. I will consider the content (text, images, audio and video) that I post to our online platform before I submit the content.

2. I will not use online platforms and services for any non-school related activity including on class chats.

3. I will be polite and courteous when communicating with other users and will use the same language as if I were talking to that person face-to-face.

4. I will adhere to the requirements of any work and not submit work in a format or on a platform not specified by my teacher.

5. Wherever possible I will undertake remote working in a public location in my house (e.g. the kitchen or living room). If this is not possible, I will try to be seated on a chair and/or at a desk.

6. I will login to Microsoft Teams by 9:30 am Monday to Friday during term time (if in Whole Bubble/Whole School Isolation).

7. If I encounter technical problems (e.g. not being able to log in to a system), I will contact the school office (01455 842047) and provide them with a detailed explanation of the problem so they can get in touch with the relevant staff members.

8. I will not, under any circumstances, try to access the accounts of any other user.

9. I understand that cyberbullying is unacceptable and will not use any online platform to undertake such activity. If I do, I will be sanctioned.

10. I understand that posting immature or offensive content to teachers or fellow pupils is unacceptable and I may be sanctioned if I undertake such action. This includes offensive or immature emojis, gifs or animations.

11. If I receive any communication or content that I am unhappy with (e.g. cyber-bullying, extreme or offensive content), I will immediately report it to the school.

12. I understand that **ALL** activity that I undertake on a school-maintained platform or a school device is monitored and logged for safeguarding and recording keeping purposes.

I have read and understood the Barwell Academy Online Remote Learning Responsible User Agreement.

Pupil Name: .....

Date.....

Bring Your Own Device Policy (BYOD)

1. INTRODUCTION

1.1 This policy contains the bring your own device policy Barwell Church of England Academy.

1.2 Barwell Church of England Academy reserves the right to amend, replace or remove the contents of this policy from time to time, in its absolute discretion. Any amendments or revisions will be notified to staff by email and subsequently incorporated into future editions.

1.3 Staff members are required to familiarise themselves with the contents of this policy and comply with it at all times.

1.4 This policy applies when staff are using their own devices on or off Barwell Church of England Academy's premises.

1.5 This policy should be read in conjunction with Barwell Church of England Academy's Online Safety Policy (including Acceptable Use).

2. PERMITTED DEVICES

2.1 Staff members are only permitted to use their own personal electronic devices, including laptops, desktops, mobile phones and tablets in the workplace for work related purposes and in accordance with this policy.

3. ACCEPTABLE USE

3.1 All personal electronic devices must be used responsibly at all times and in accordance with Barwell Academy's data protection policy and the general rules regarding the use of IT equipment, as set out in Barwell Church of England Academy's online safety policy.

3.2 Devices that are not approved in accordance with this policy must not be used to connect to the Barwell Academy network.

3.3 Staff members must not use the camera and/or video functionalities to take images/footage of children whilst they are using their personal devices on Barwell Church of England Academy premises.

3.4 Barwell Church of England Academy may monitor the use of its IT systems even where such use occurs through personal devices authorised for work related activities in accordance with this policy. Any such monitoring will be carried out in accordance with Barwell Church of England Academy's online safety and its Data protection policy.

4. SECURITY

4.1 All personal electronic devices must be password protected using a six-digit pin or biometric entry.

4.2 If left idle for five minutes, devices must be set to lock themselves with their pin or biometric entry.

4.3 Staff members must ensure that personal devices used for work activities are updated with the latest software and that encryption and anti-virus protection is activated (where relevant).

4.4 To enable devices to be wiped remotely in event of loss, theft or damage, relevant software to track and/or wipe devices must be installed and configured (where appropriate).

4.5 If a device that has been authorised and used for work related purposes in accordance with this policy is lost, stolen or damaged, staff members must report this to Rachael Peace (DPO) as soon as they become aware of the loss, theft or damage.

4.6 Barwell Church of England Academy assumes no liability for any losses incurred as a result of the loss, theft or damage to a staff member's personal device.

5. DATA PROTECTION

5.1 All staff members must comply with the Barwell Church of England Academy data protection policy at all times.

5.2 Staff members must not store any personal data obtained or processed during the course of their work activities on their personal devices.

5.3 Any personal data that is processed using staff members' personal devices must be dealt with and subsequently deleted in accordance with Barwell Church of England Academy data protection policy.

5.4 In the event that Barwell Church of England Academy receives a data subject access request, staff members may be required to provide Barwell Church of England Academy with access to personal devices that have been used for work activities in order to retrieve and/or review any relevant personal data about the individual who has made the request. Staff members must cooperate with Barwell Church of England Academy and carry out reasonable searches for such information.

6. BREACH OF THIS POLICY

6.1 All staff members (including employees, casual workers, officers and agency workers) must comply with this policy. Any breach of this policy will be taken extremely seriously and, in the case of employees, may lead to disciplinary action up to and including dismissal.

7. END OF EMPLOYMENT OR HIRE

7.1 Before leaving the Barwell Church of England Academy, staff members must ensure that all data and information relating to Barwell Church of England Academy activities is deleted from their personal devices.

Signed: ……

Barwell Church of England Academy

24th May 2021