Bretherton Endowed CE Primary School Filtering Policy

"Walking in the footsteps of Jesus with our Christian family, we learn, grow, achieve and flourish together in God's love."

This policy is for Bretherton Endowed CE Primary School and The Hub, Bretherton Endowed Out of School Provision.

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Head teacher with the support of Virtue Technology.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities.

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- Appropriate security measures are in place (See Appendix 1) to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (See Appendix 2)
- All users will have clearly defined access rights to school technical systems.(See Appendix 3)
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (see password section below)
- The school bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place (See Online safety policy)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (See Appendix 4)
- Remote management tools are used by senior staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Network (See Appendix 5 5:1)
- An agreed policy is in place (See Appendix 6 6:1) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place (6:2) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place (6:3) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (See Appendix 7) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All school / academy networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users will be allocated by request to Virtue Technology. This will be recorded in the 'events log' in Appendix 8.
- Users will change their passwords at regular intervals

Staff Passwords

- All staff users will be provided with a username and password by Virtue Technology technician who will keep the up to date record of users and their usernames updated in school office.
- the password should be a minimum of 8 characters long and must include – uppercase character, lowercase character, number and/or special characters
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 60 to 90 days and should not re-used for 6 months and be significantly different from previous passwords created by the same user.

Student / Pupil Passwords

- Previously children were allocated a username and password allocated by Virtue for access to a windows device. Bretherton Endowed in conjunction with parents have rolled out a chromebook 1 to 1 device scheme. This means that children no longer require a windows network login. (See Google admin section below)

- Children will continue to be taught the importance of password security

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- staff meetings and regular updates
- through the Acceptable Use Agreement

Children will be made aware of the school's password policy:

- in computing lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (Head Teacher) will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

We will:

- use the provided filtering service without change or but allow flexibility for sites to be added or removed from the filtering list for their organisation
- No differentiated filtering for different ages of users will be provided

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Head teacher along with the Online Safety Governor. They will manage the school filtering, in line with this policy and will keep records of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must :

- be logged in change control logs
- be reported to a second responsible person (Online Safety Governor via termly report)

All users have a responsibility to report immediately to The Head teacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering systems in place to prevent access to such materials. Such reference is made to the Mobile phone policy.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider - NetSweeper
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head teacher and the details will be documented for the online safety governor termly report.

Education / Training / Awareness

Children will be made aware of the importance of filtering systems through the online safety education programme included in our computing curriculum.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / website links, newsletter etc.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering the grounds on which they may be allowed or denied
- the use of the Governotr termly report as a log of changes
- any audit / reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Headteacher who will decide whether to make school level changes. The Headteacher, Deputy Head Teacher and Computing lead are staff in school with access to the Admin area of Netsweeper.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:*

- *Termly reports to governors from Netsweeper filtering service listing breaches and recording key areas of concern.*
- *Weekly reports sent from Netsweeper identifying IP address and content filtered or declined.*
- *Observational supervision of children during in class activities.*
- *Routine (at least half termly) class teacher checks on history and recent searches.*

- *One off searches of history if alert to concerns.*

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Onliine Safety Governor via termly reports) which will feed into curriculum and standards committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

We have sought guidance: *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

KCSE *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

Adopted : March 2023

To be reviewed :No later than the end of 2025

All aspects of our policy intends to comply within the Data Protection (GDPR) legislation.

Appendix 1

Appropriate secutity measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data through:

- Height of hardware
- Lockage cabinet
- Password protected sites
- Security of passwords in place
- Policy for personal data equipment

Appendix 2

Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff

Overall security manager: Head teacher
Second : Online Safety Governor
Support in school through bought in service: IT Solutions. Matthew Schofield
Local Authority support/advice: BTLS Lancashire

Appendix 3 –

Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.

Access Rights	Name
Administrator	Headteacher
	Matt Schofield
Staff rights	All school staff including Bursar
Children	Restricted rights

Appendix 4:

School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

Date	*Random audit of use involving:*	*Outcomes/action*

Appendix 5:

5:1 An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator

On identification of an actual/potential technical incident, the informant must report to Head teacher using the potential breach form (See Online Safety Policy)

Incidents involving adults

- Close computer if appropriate
- Pass information toHeadteacher, DHT or school office using reporting form
- Head teacher to follow protocol in Online safety policy

Incidents involving children

- Establish the facts and close the computer without deleting/ closing the package
- Remove the computer and child from the area
- Pass the computer to the Headteacher to ascertain the facts for reporting
- Speak to child and support as required, reminding them of safeguarding responsibilities
- Contact parents
- Complete safeguarding incident report for accurate reporting to governors
- Depending on the severity of incident, contact online safety governor

Appendix 6

6:1 An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system

- Log in for guests/ students will be provided.
- Only 1 guest user name and password will be used at any time and diary entry of who using to support investigation of possible future breach
- Additional monitoring may be required at periods of additional guests/visitors using our network
- Guest internet log in supports additional filtering/ monitoring should we require it.

6:2 An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users

- Staff should not download any files or programmes that are saved onto the school server. Minor files can be downloaded and saved onto individual computers, however if in any doubt as to the validity of the programmes, advice MUST be sought.

6:3 An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

Appendix 7

An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy Template in the appendix for further detail)

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office . for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require

Commissioner’s Office website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including children, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, children progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is the Head Teacher. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) -School business officers for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information as been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through display in entrance hall and on school website. Parents / carers of young people who are new to the school will be provided with the privacy notice through their welcome pack.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through: Induction training for new staff

- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
Not Protectively Marked	0	Will apply in schools
Protect	1 or 2 mostly in schools	
Restricted	3	
Confidential	4	Will not apply in schools
Highly Confidential	5	
Top Secret	6	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g.. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly.User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software, and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation. A destruction log is kept in school office.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate_data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or

	personalised curriculum and educational needs.	communication to a personal device or email account belonging to the parent.	higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendices: Additional issues / documents related to Personal Data Handling in Schools:

Use of Biometric Information

Parental permission for use of cloud hosted services

Currently Bretherton doesn't operate a cloud based system.

Schools that use cloud hosting services (eg.Google Aps for Education) may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent'. Normally, schools will incorporate this into their standard acceptable use consent forms sent to parents each year (see suggested wording on "Parent / Carer Acceptable Use Agreement Template").

A template form has been added to the Parents & Carers Acceptable User Template elsewhere in these Template Policies.

Privacy and Electronic Communications

Schools should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Freedom of Information Act

All schools (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- Ensure that a well-managed records management and information system exists in order to comply with requests

- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy Trust to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioners Office provides schools and academies with a model publication scheme which they should complete. This was revised in 2009, so any school with a scheme published prior to then should review this as a matter of urgency. The school's publication scheme should be reviewed annually. (see separate Model Publication Scheme)

Appendix - DfE Guidance on the wording of the Privacy Notice

Bretheton Endowed CE Primary School

Privacy Notice - Data Protection Act 1998

We Bretheton Endowed CE Primary School are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact the school office.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites: http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Public Communications Unit, Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk

Email:	http://www.education.gov.uk/help/contactus
Telephone:	0370 000 2288

Appendix 8

Events log

Date	Staff	Event description	Comments	Signed off