Policy adopted: May 2018
Policy reviewed: May 2018
Next Review date: May 2019
Designated SLT Link: Colin Belford
Archway School has a duty to monitor the operation and effectiveness of policies. Designated authority: Governors Finance, Staffing & General Purposes Committee

Archway

Data Protection Policy

Contents

Appendices:

1. Aims

Our school aims to ensure that all data about staff, students, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998, and the General Data Protection Regulation (GDPR), which comes into effect in May 2018.

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force in 2018.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our school processes personal information relating to students, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Data Protection Officer, Mr Mervyn Murray

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- data shall be processed fairly and lawfully
- personal data shall be obtained only for one or more specified and lawful purposes
- personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- personal data shall be accurate and, where necessary, kept up to date
- personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the Headteacher, or the Data Protection Officer in the Headteacher's absence. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Privacy/fair processing notice

7.1 Students and parents

We hold personal data about students to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about students from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- contact details

- results of internal assessment and externally set tests
- data on student characteristics, such as ethnic group or special educational needs
- exclusion information
- details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about students with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

Once our students reach the age of 13, we are legally required to pass on certain information to Gloucestershire County Council, which has responsibilities in relation to the education or training of 13-19 year-olds. Parents, or students if aged 16 or over, can request that only their name, address and date of birth be passed to Gloucestershire County Council by informing Data Protection Officer.

We are required, by law, to pass certain information about students to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- enable individuals to be paid
- facilitate safe recruitment
- support the effective performance management of staff
- improve the management of workforce data across the sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring
- support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- contact details
- National Insurance numbers
- salary information
- qualifications
- absence data
- personal characteristics, including ethnic groups
- medical information
- outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Data Protection Officer.

7.3 Other Adults & Volunteers

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school including to:

- enable individuals to be paid
- facilitate safe recruitment
- support the effective performance management of staff
- improve the management of workforce data across the sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring
- support the work of the School Teachers' Review Body

This data includes, but is not limited to, information such as:

- contact details
- National Insurance numbers
- personal characteristics, including ethnic groups

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.
We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Data Protection Officer.

8. Subject access requests

Under the Data Protection Act 1998, individuals have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- the individual's name
- a correspondence address
- a contact number and email address
- details about the information requested

The school will not reveal the following information in response to subject access requests:

- information that might cause serious harm to the physical or mental health of the student or another individual
- information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- information contained in adoption and parental order records
- certain information given to a court in proceedings concerning the child

If a subject access request does not relate to an educational record, we will respond within 1 month of receipt of the request. We will provide the information free of charge.

When responding to requests we may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs.

A request will be deemed unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9. Parental requests to see the educational record

Parents/carers have the right of access to their child's educational record under the Pupil Information Regulations (PIR) 2005, but any other information we may hold falls within the remit of the Data Protection Act (DPA) 1998, and within the remit of the General Data Protection Act (GDPR) when that comes into force on 25 May 2018.

Please bear in mind the Information Commissioner's Office, which is the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand the implications of holding personal information or releasing that information to anyone. If parents/carers wish to make a request under the DPA or the GDPR, they should provide a statement from their child stating they are aware of what personal information is, and that parents/carers are asking to see this information.

The school will respond to a request made under the PIR within 15 school days, and within 40 calendar days for requests made under the DPA. This will reduce to within one calendar month for requests made under the GDPR. While we will not charge parents/carers for making a request, we may ask them to cover the cost of copying the information (the disbursement costs) if there is a large quantity.

10. Storage of records

- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access

- Passwords must contain a minimum of 8 characters and must include 3 of uppercase character, lowercase character, number and special character. This does not apply to students
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

12. Maintenance of up to date data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined. We hold student data until the student reaches 25 years of age. SEN files are held for 30 years from a student's date of leaving. We hold school workforce data for the time specified in the Information and Records Managements Society Retention Guidelines for Schools.

13. Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. If the data is found to be wrong, incomplete or inaccurate, it will be amended accordingly. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

14. Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous and clearly decipherable and readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

15. Training

Our staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

16. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018. We will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

17. Monitoring arrangements

- The Headteacher is responsible for monitoring and reviewing this policy
- The Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records yearly
- This document will be reviewed when the General Data Protection Regulation comes into force, and then **every year**

18. Photographs

Whether or not a photograph comes under the Data Protection Act 1998 is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely seriously. The school will seek to obtain parents' permission for the use of photographs outside the School and will record their wishes if they do not want photographs to be taken of their children.

19. Links with other policies

This data protection policy and privacy notice is linked to:

- Freedom of Information Policy
- Internet and Computer Usage Policy – Staff, Other Adults and Volunteers
- Internet and Computer Usage Policy – Students
- Equalities Policy
- Safeguarding Policy

APPENDIX 1

Privacy Notice (How we use student information)

The categories of student information that we collect, hold and share include:

- personal information (such as name, unique student number and address)
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- attendance information (such as sessions attended, number of absences and absence reasons)
- assessment information
- relevant medical information
- special educational needs information
- exclusions / behavioural information
- post-16 learning information

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to make statutory returns to the LA and Government Departments

The lawful basis on which we use this information

We collect and use student information under the Education Act 1996. The EU General Data Protection Regulation 2016/679 (GDPR) will take effect in May 2018 including Article 6 'lawfulness of processing' and Article 9 'processing of special categories of personal data'.

https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

We hold student data until the student reaches 25 years of age. SEN files are held for 30 years from a student's date of leaving.

Who we share student information with

We routinely share student information with:

- schools that the students attend after leaving us
- our local authority
- the Department for Education (DfE)
- School Nurse

We also provide student level personal data to third party organisations which supply services to us for which the provision of the data is essential for the service to be provided. We currently provide student level data for the following purposes:

- systems integral to the delivery of core business services, eg Capita SIMS, 4Matrix, Mintclass
- systems integral to the operation of IT services systems, eg Smoothwall, Microsoft, Salamander
- curriculum products, eg GCSE Pod, Show My Homework, PIXL Edge, itslearning

A full list is available upon request.

School staff and invited representatives of the press do take photographs of students, in school or on school trips, for internal purposes. We may use these photographs for publication, for school publicity, but we will not name the students without the consent of their parents.

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or carer can request that *only* their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child/student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe**Requesting access to your personal data**

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mervyn Murray, Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:
Mervyn Murray, Data Protection Officer – email: mervynmurray@archwayschool.net

APPENDIX 2

Privacy Notice (How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, address, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information
- other payroll information (such as bank sort code and account number)

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid

The lawful basis on which we process this information

We process this information under the Education Act 1996. The EU General Data Protection Regulation 2016/679 (GDPR) will take effect in May 2018 including Article 6 'lawfulness of processing' and Article 9 'processing of special categories of personal data'.
https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for the time specified in the Information and Records Managements Society Retention Guidelines for Schools.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

We also provide personal data to third party organisations which supply services to us for which the provision of data is essential for the service to be provided. We currently provide personal data for the following purposes:

- systems integral to the delivery of core business services, eg Capita SIMS, 4Matrix, Mintclass

- systems integral to the operation of IT services systems, eg Smoothwall, Microsoft, Salamander
- Curriculum products, eg GCSEPod, Show My Homework, itslearning

A current list is available on request.

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required

- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Mervyn Murray, Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact: Mervyn Murray, Data Protection Officer
Email: mervynmurray@archwayschool.net

APPENDIX 3

Data Backup and Retention Procedures

Introduction

The school follows the industry recommended "3-2-1 Backup Strategy" which means 3 total copies of data, 2 of which are on different mediums, and one offsite or relocated.

The three copies are Storage snapshots, backup to disk and backup to tape. The two mediums are disk based backups and tape backups. The relocated data is stored on tapes in a fireproof safe in a separate part of the building. For added coverage, the disk backups are also stored in a different building to the live data and storage snapshots.

Scope

The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as key deliverable and is not therefore designed as a method of archiving material for extended periods of time.

The 'data' backups covers all systems managed by the IT department. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IT. All critical data must be stored on the network drives provided or on central email services. Where this is not possible, individuals are reminded that they are personally responsible for data held locally on their desktop, laptop or other electronic devices.

Backup Policy

- Where possible backups are run overnight and are completed before 8am on working days
- Upon completion of backups, media copies are moved to a secure fireproof safe for disaster recovery purposes
- A limited number of authorised personnel have access to the backup application and media copies
- Requests for backup data from 3rd parties must be approved by the Head teacher
- Backup of data held within MIS Systems have data backup routines which ensure database integrity is retained. Other systems are able to backup data on- line whilst maintaining data integrity
- The IT Backup systems have been designed to ensure that routine backup operations require no manual intervention
- The IT department monitor backup operations and the status for backup jobs is checked on a daily basis during the working week
- Any failed backups are re- run immediately the next working day

Restore

- Data is available for restore within a few minutes of a backup job completing daily schedule
- Data will be available during the retention policy of each backup job – which is currently defined as 3 months
- Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IT systems at Archway School have been specified to minimise data loss between backup

windows by having elements of system redundancy

- Requests for data recovery should be submitted to the IT help desk

Backup Retention Policy

Storage Snapshots:

Storage snapshots are taken every weekday with a retention of five snapshots, and weekly with a retention of 12 snapshots. Covering a total of 5 months for dailies and 3 months for weeklies.

Disk Backups:

A full backup is taken to disk once per month. Two full backups sets are stored. Then taken incrementally daily with a retention of 31 copies.

Tape Backups:

The latest full disk backups are taken to tape every weekend along with the preceding week of incremental backups. There are four backup sets comprising of one full backup each. Retained for 1 month.

APPENDIX 4

Technical Security Procedures (including filtering and passwords)

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/network 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 procedure
- 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 IT Manager

Technical Security

Procedure statements

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- 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 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 (IT Manager and Technicians)
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the IT Manager / Technical Staff (or other person) and will be reviewed, at least annually
- Users will be made responsible for the security of their username and password and 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.
- The IT Manager 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.
- School technical staff will regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity

- An appropriate system is in place (AUP) for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).
- An agreed procedure is in place (through reception staff) 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 (AUP) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place (AUP) 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 (AUP) 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. (see School Personal Data Procedure)

Password Security

A safe and secure username/password system is essential 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 IT Manager (or other person) and will be reviewed, at least annually.
- All school 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. Consideration will be given to using two factor authentication for such accounts.
- All users 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.
- Where passwords are set/changed manually requests for password changes should be authenticated by (IT Services) to ensure that the new password can only be passed to the genuine user

Staff Passwords

- All staff users will be provided with a username and password by the IT Manager or technicians who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- 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 year
- should not re-used for at least 6 months and be significantly different from previous passwords created by the same user. The last four passwords cannot be re-used.

Student Passwords

- All students will be provided with a username and password by the IT Manager or technicians who will keep an up to date record of users and their usernames.
- Students will not be required to change their password.
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Awareness

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

- at induction
- through the Acceptable Use Policy

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

- in lessons
- through the Acceptable Use Policy

Audit/Monitoring/Reporting/Review

The IT Manager 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 procedure

<u>Filtering</u>

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. 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.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the IT Manager. They will manage the school filtering, in line with this policy and will keep records / logs 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 (the Head Teacher)

All users have a responsibility to report immediately to the IT Manager 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 / security systems in place to prevent access to such materials.

Policy Statements

- Internet access is filtered for all users
- Illegal content is filtered by Smoothwall and 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
- The school has provided enhanced/differentiated user-level filtering through the use of the Smoothwall filtering programme, allowing different filtering levels for different ages/stages and different groups of users – staff/students etc.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader)
- 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 IT Manager
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager/technicians

Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

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

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

Parents will be informed of the school's filtering procedure through the Acceptable Use Policy and through online safety awareness sessions / newsletter etc.

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 Policy.

Audit / Reporting

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

- the second responsible person (Head Teacher)
- 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

Schools in England (and Wales) are required *"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).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to *"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/

APPENDIX 5

Student Starters and Leavers

New Student Starters

The Data Manager/Headteacher's PA will inform the IT Manager of any new students and their start date.

1. Computer account is created and set to auto-enable on the first day in school
2. Accounts are created for Active Directory, Email, Papercut and Cashless Catering
3. Students are given their login information by their tutor

Student Leavers

The Data Manager/Headteacher's PA will inform the IT Manager of the name, tutor group and leaving date of the student.

1. Computer account is set to automatically disable at midnight on the final day in school.
2. After the final day that the student is in school the student is then removed from:
    a. Active Directory
    b. School email
    c. Papercut
    d. Cashless Catering database
    e. Parentmail

Data Backup

Backups of any student leavers work areas are kept for 5 years.

APPENDIX 6

Staff Starters and Leavers

New Staff Starters

The Business Manager will inform the IT Manager of any new staff and their start date.

1. Computer account is created and set to auto-enable on the first day on their employment
2. Accounts are created for Email, SIMS, Internet Unfiltered Access, Door Access, Papercut and Cashless Catering (if requested)
3. Staff are given their login information during their IT induction and are also emailed a welcome pack of useful help documents and issued with a security pass

Changes in Staff Job Roles

The Business Manager will inform the IT Manager of any changes to staff job roles.

1. Depending on the role, the member of staff will need modified levels of access to various systems (SIMS, file permissions, email groups etc.)

Staff Leavers

The Business Manager will inform the IT Manager of the name and leaving date of the member of staff.

1. Computer account is set to automatically disable at midnight on the final day of their employment
2. Before their employment ceases, staff are asked to:
    a. Return their security pass
    b. Return their staff laptop
    c. Return their encrypted USB
    d. Sign a declaration that they have no student information on devices outside of school
3. After the final day of the staff leaver's employment the member of staff is removed from
    a. Active Directory
    b. SIMS
    c. Internet Unfiltered Access
    d. Door Access
    e. Papercut
    f. Cashless Catering database

Annual Audit

The IT Manager will carry out an annual audit with the Headteacher's PA in September of new staff, leavers and any job changes.

APPENDIX 7

Personal Data Handling

Introduction

The School and its 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 Commissioner's 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, regulations and guidance (where relevant from the Local Authority).

Responsibilities

The Headteacher and the Data Protection Officer 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): The Data Manager/Student Services Manager for student and assessment data and the Business Manager for Staff data. 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 has 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.

Information to Parents/Carers – the "Privacy Notice"

In order to comply with fair processing requirements, the school will inform parents/carers of all students of the data they collect, process and hold on them, the purposes for which the data is held and the third parties to whom it may be passed. This privacy notice will be issues to parents/carers via electronic mail/letter and will be published as part of this policy in the policy section of the school website. Parents/carers of young people who are new to the school will be provided with the privacy notice in their starter pack.

Training & Awareness

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

- Induction training
- Meetings/briefings/Inset
- Day to day support and guidance from Information Asset Owners, Data Protection Officer the Headteacher and members of the SLT

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners and/or Data Protection Officer 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)
- Prioritising the risks

The following risks have been identified and categorised (see Appendix Z below for Government Guidelines on Protective Marking):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Like-lihood	Overall risk level (low, medium, high)	Action(s) to minimise risk
1	Student personal contact data	Data Manager/ Student Services Manager	2	Low	Low	Password protocol/tiered and restricted access
2	Staff personal contact data	Business Manager	2	Low	Low	Password protocol/tiered and restricted access
3	Staff data eg absence/PDA	Business Manager	2	Low	Low	Password protocol/tiered and restricted access
4	Student assessment data	Data Manager	2	Low	Low	Password protocol/tiered and restricted access

Impact Levels and protective marking

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.

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 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 eg. "**When you have finished with it, this document should be added to one of the secure storage facilities for confidential information for destruction; these are located in the Data Office, Main Office, Finance and Reception**".

Secure Storage of and access to data

The school will ensure that ICT 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.

Personal data may only be accessed on machines that are securely password protected.

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 (ie owned by the staff, governors, etc.) 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/device must be encrypted and password protected,
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), 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.

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

Archway School has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, 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, Archway 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 with the exception of school trips where the material is the responsibility of the trip leader.

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 use secure remote access to school systems;
- 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
- 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. This retention/destruction of personal data and confidential school information will comply with the Retention Guidelines document provided for schools by the Information and Records Management Society.

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 or be disposed of through an approved third party.

Documents for destruction by an approved third party will be added to one of the secure storage facilities for confidential information for destruction. These storage facilities will be emptied by either the Site Manager or Assistant Site Manager and disposed of through that approved third party; certificates of secure destruction will be retained by the Business Manager.

It is recognized that the Site Manager and Assistant Site Manager will have contact with confidential personal/organisational material etc in the course of their duties. It is the Site Manager's responsibility to ensure that the emptying of secure disposal storage is restricted to the him/herself and the Deputy Site Manager with the understanding that contents of such files must be kept confidential.

Audit Logging/Reporting/Incident Handling

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. All incidents will be logged with the IT Manager/Data Protection Officer

In managing and recovering from information risk incidents, the following will be established:

- a “responsible person” for each incident
- a communications plan, including escalation procedures
- a plan of action for rapid resolution
- a plan of action of non-recurrence and further awareness raising

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

Appendix Z – Government Guidelines on Use of technologies and Protective Marking

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in Archway School
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	**May apply in Archway School eg some meeting minutes**
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	Will not apply in schools

Most student or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The following is 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 publicly 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 personalised curriculum and educational needs.	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 communication to a personal device or email account belonging to the parent.	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 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.