MONKSEATON HIGH SCHOOL
DATA PROTECTION POLICY

Including:

- **Data Protection Policy Statement**
- **Data Protection Policy**
- **Data Breach Reporting Policy**
- **Biometric Information Policy**

Status:

Statutory policy or document	No
Review frequency	Bi-Annually
Approval by	Governing Body
Approval date	7th February 2024

Publication:

Statutory requirement to publish on school website	No
Agreed to publish on school website	No

Review:

Frequency	**Next Review Due**
Every two years	Feb 2026

Version Control:

Author	**Creation / Revision date**	**Version**	**Status**
Business Manager (SP)	March 2018	1.0	Final approved version for publication. Using Information Governance Team Model Policy Version 1.0
Business Manager (MAD)	10.05.2023	2.0	Completely re-written using Information Governance Team Model Policy Version 4.0. Data Protection Policy Statement, Data Protection Policy, Data Breach Policy and Biometric Information Policy combined into one document.
Business Manager	18.01.24	2.1	Review – minor formatting changes. Updated reference to parent / carer throughout. Updated biometric information.

DATA PROTECTION POLICY STATEMENT

Monkseaton High School is fully committed to full compliance with the requirements of the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018. The School will therefore follow procedures which aim to ensure that all our staff, Governors, and contractors who have access to any personal data held by or on behalf of the School are fully aware of and abide by their duties under the data protection legislation. We also adhere to the guidance issued by the Information Commissioner.

Policy Statement
We collect and use information about our students in order to carry out our functions. This also includes information about current, past and prospective staff, students and parents/carers and suppliers of services to us. In addition, we are required by law to collect and use information in order to comply with statutory requirements. Personal information must be processed appropriately irrelevant of how it is collected, recorded or used and in whatever format it is held.

We regard the handling of personal information as very important to us being able to carry out our day-to-day business and essential to maintaining confidence. We therefore fully adhere to the Principles of the UK GDPR.

How we handle personal and sensitive data
We will ensure that appropriate controls and measures are in place to monitor and review data so:

- It is secure and protected.
- It is used in efficient and effective ways to improve the education of our students.
- Only necessary data is collected.
- It is only collected for the purpose as described at the time of collection.
- Information is accurate.
- Information is not kept for longer than is necessary.
- Data which is no longer needed is securely destroyed.
- Information is not transferred abroad without suitable safeguards.
- There is general information for students and parents/carers and staff of their rights to access information.
- The rights of students, parents/carers and staff about whom information is held can be fully exercised under the UK General Data Protection Regulations.

We will also ensure appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data) are in place.

Individual rights

Under Data Protection Legislation individuals have the right to:

- Request access to their own personal information within one month of request.
- Prevent processing of their information in certain circumstances.
- Request that information be corrected, rectified or blocked where it is identified as incorrect.
- Expect that we have an officer specifically responsible for data protection in the School.
- Expect guidance and training for staff is provided at an appropriate level.
- Ensure that any breaches of this policy are dealt with appropriately and in a timely manner.

The Principles of Data Protection

The UK GDPR stipulates that anyone processing personal data must comply with 7 key principles of good practice. The key principles are legally enforceable and consist of

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability.

For more information about the key principles, citizens' rights and the distinction between personal data and 'special categories' under Data Protection legislation please see the Information Commissioners Data Protection Pages.

If you would like to know more about how we use your information, please contact the school office or our Data Protection Officer at the following:

email: dpo.schools@northtyneside.gov.uk

Data Protection Officer for Schools
Information Governance Manager
Law and Governance
North Tyneside Council
The Silverlink North
Cobalt Business Park
NE27 0BY

DATA PROTECTION POLICY

1. Introduction

Monkseaton High School Data Protection Policy has been produced to ensure compliance with UK General Data Protection Regulation (UK GDPR) and associated legislation and incorporates guidance from the Information Commissioner's Office (ICO).

The Data Protection Policy gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

Monkseaton High School is registered with the ICO as a Data Controller for the processing of living individuals' personal information. (ICO registration number: **Z7747721**).

2. Purpose

Monkseaton High School Data Protection Policy has been produced to ensure its compliance with UK GDPR.

The Policy incorporates guidance from the ICO and outlines the School's overall approach to its responsibilities and individuals' rights under the data protection legislation.

3. Scope

This policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the School), third parties and others who may process personal information on behalf of the School.

The policy also covers any staff and students who may be required to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the School to ensure the data is processed in accordance with UK GDPR and that students and staff are advised about their responsibilities.

4. Data covered by the Policy

A detailed description of this definition is available from the ICO, however briefly; personal data is information that relates to an individual and the individual can be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual. This includes data held manually and electronically and data compiled, stored or otherwise processed by the School, or by a third party on its behalf.

Special category data is personal data that is more sensitive in nature and requires a higher level of protection. This consists of information relating to:

- race
- ethnic origin
- politics
- religion
- trade union membership

- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation.

5. The seven data protection principles

UK GDPR requires Monkseaton High School, its staff and others who process or use any personal information to comply with the seven data protection principles.

The principles require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals.
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) accurate and, where necessary, kept up to date.
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
g) accountability, the controller shall be responsible for, and be able to demonstrate compliance with all of the above.

6. Responsibilities

Monkseaton High School has an appointed Data Protection Officer to handle day-to-day issues which arise, and to provide members of the School with guidance on Data Protection issues to ensure they are aware of their obligations.

Employees of Monkseaton High School are expected to:

- Familiarise themselves and comply with the seven data protection principles.
- Ensure any possession of personal data is accurate and up to date.
- Ensure their own personal information is accurate and up to date.
- Keep personal data for no longer than is necessary, in line with retention guidelines.
- Ensure that any personal data they process is secure and in compliance with the School's information related policies and strategies.
- Acknowledge data subjects' rights (e.g. right of access to *all* their personal data held by the School) under UK GDPR, and comply with access to those records.
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the School.
- Contact dpo.schools@northtyneside.gov.uk for any concerns or doubt relating to data protection to avoid any infringements of the data protection legislation.

Students, of Monkseaton High School are expected to:

- Comply with the seven data protection principles
- Comply with any security procedures implemented by the School.

7. Obtaining, disclosing and sharing

Only personal data that is necessary for a specific School related business reason should be obtained.

Students and their parents/carers will be informed about how their data will be processed.

Upon acceptance of employment at Monkseaton High School, members of staff will also be informed about the processing and storage of their data which is required as part of their legal contract and employment legislation.

Data must be collected and stored in a secure manner.

Personal information must not be disclosed to any third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the School. The only exception to this is where the School has safeguarding concerns (please see paragraph 9.0).

Monkseaton High School may have a duty to disclose personal information in order to comply with legal or statutory obligations. UK GDPR allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purpose and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the data protection legislation.

8. Retention, security and disposal

Those responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform the School.

Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with Article 5 of UK General Data Protection Regulations, personal information shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of UK GDPR, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its

secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

Monkseaton High School's staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

All data past its retention period should be destroyed in accordance with the retention schedule when it is no longer required.

Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data held in electronic format should be deleted. Hardware or any digital storage devices should be appropriately disposed of in compliance with the ICT service provider contract and conform with UK GDPR requirements.

The four categories of retention periods to be applied to data are as follows:

a) One month after the creation of the data, to ensure any 'loose ends' are tied up.
b) One year after the student to whom the data relates leaves the School, in order to ensure smooth handover activity to any subsequent school.
c) Five years after the student to whom the data relates leaves the School, to support longer term analysis of progress, attainment, support for different student groups etc.
d) Until the child is 25 years of age or older, in instances where detailed information about activities in school may form part of safeguarding for that individual.

Where Monkseaton High School decides to retain data for 5+ years, it will take steps to de-personalise it as time goes on. For example, names can be replaced with initials or other pseudonymisations.

9. Safeguarding

UK GDPR does not prevent the sharing of information for the purposes of keeping children safe. The Data Protection Act 2018 allows for schools to process sensitive information without consent where there are safeguarding concerns.

If Monkseaton High School decides to share information for safeguarding purposes, the Designated Safeguarding Leads must record who they are sharing the information with and for what reason. If it is appropriate to do so, they should seek the consent of the data subject. If consent is not sought, this decision must be recorded.

10. Transferring personal data

Any transfer of personal data must be done securely in line with Monkseaton High School Information Security procedures:

Email communication is not always secure and sending personal data to external emails should be avoided unless it is encrypted with a password provided to the recipient by separate means.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly, and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purposes.

11. Data Subjects Right of Access (Subject Access Requests) Education Regulations
Under data protection, individuals (both staff and students) have the right of access to their personal data held by the School. This applies to data held in both paper and electronic format, and within a relevant filing system.

Monkseaton High School shall use its discretion under UK GDPR to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

Any individual who wishes to exercise this right should make the request in writing by contacting office@monkseaton.org.uk / 01912979700.

Monkseaton High School will not charge a fee. It will only release information upon receipt of a written request along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the necessary documentation.

12. The Education (Student Information) (England) Regulations 2005 – Information Request
Under education regulations, those with parental responsibility can request access to a child's education record. Access to education records is a separate right and is not covered by Data Protection legislation.

An education record covers information that comes from the school, the student or the parent, and is processed by or for the school's Governing Body or teacher. This is likely to cover information such as the records of the student's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's Governing Body. It may also include information from the child and parent, carer or guardian.

Information provided by the parent/carer of another child or information created by a teacher solely for their own use would not form part of a child's education record.

Those with parental authority will be able to view the record free of charge within 15 school days of the request.

If there is a request for a copy of the record, we can charge a fee for this, however, the fee will not exceed the cost of supplying the records. This will also be provided within 15 school days.

13. Reporting a data security breach

It is important Monkseaton High School responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on school systems, and unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the Data Protection Officer at dpo.schools@northtyneside.gov.uk and if it relates to an IT incident (including information security), should also be reported to the Headteacher.

Any breach will be investigated in line with the procedures within the UK GDPR. In accordance with that policy, Monkseaton High School will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

DATA BREACH REPORTING POLICY

1. Introduction

Monkseaton High School holds, processes and shares a large amount of personal data, a valuable asset that needs to be protected.

Every care is taken to protect personal data and avoid a data protection breach (either accidental or deliberate).

Compromise of confidentiality, integrity, or availability of information may result in harm to individuals, reputational damage, a detrimental effect on service provisions, legislative non-compliance and financial costs.

2. Purpose

Monkseaton High School is obliged, under the Data Protection Legislation, to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breaches and information security incidents across the school.

3. Scope

This policy relates to all personal data held by the School regardless of format.

This policy applies to all staff and contractors at the school. This includes teaching staff, temporary, casual and agency staff, suppliers and data processors working for or on behalf of the school.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what remedial action is necessary to secure personal data and prevent further breaches.

4. Definition / types of breach

An incident, in the context of this policy, is an event which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberate and has caused or has the potential to cause damage to the school's information assets and/or reputation.

An incident includes but is not restricted to, the following:

- Loss or theft of personal data or equipment on which such data is stored (e.g. loss of a laptop, iPad/Tablet, mobile device or paper record).
- Unauthorised use, access to (either successful or failed) or modification of data or information systems.
- Unauthorised disclosure of personal data (either deliberate or accidental).
- Offences where information is obtained by deceiving the organisation who holds it.

5. Reporting an incident

Any individual who accesses, uses or manages the school's data is responsible for reporting any data breach and information security incidents immediately to the Business Manager. If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable.

The incident should be recorded on a data breach log, which should include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, how many people are involved, and, following the investigation, information on how similar incidents will be avoided in the future.

The school's Data Protection Officer (DPO) can be contacted at dpo.schools@northtyneside.gov.uk or 0191 643 2333 for advice and guidance.

6. Containment and recovery

The designated person will firstly determine if the breach is still occurring and if so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made with relevant officers to establish the severity of the breach and who will take the lead in investigating the breach (this will depend on the nature of the breach; in some cases it could be the DPO).

Containment of the breach may involve requesting that the recipient of information that has been mistakenly disclosed, returns or deletes this document.

7. Investigation, risk assessment and notification

An investigation will be undertaken by the designated person immediately and where possible within 24 hours of the breach being discovered/reported.

This person will investigate the breach and assess the risks associated with it, for example, the potential adverse effects for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- The type of data involved
- It's sensitivity
- The protection in place (e.g. encryption)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to illegal or inappropriate use
- Who are the affected individuals, the total number affected and the potential effects on those data subjects
- Whether there are wider consequences to the breach.

The above investigation points will help determine whether the data subject/s need to be made aware of the breach, and if it needs to be reported to the Information Commissioner.

If the breach is likely to adversely affect individuals, then we will notify the data subjects without undue delay. This notification will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the school for further information.

If it is felt that the risks to individuals are high, the ICO will be contacted, with all of the above information, within 72 hours of discovering the breach.

Consideration will be given as to the necessity to notify third parties such as the Police, insurers and banks. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

Consideration will also be given as to whether any press release may be required.

All actions will be recorded on the data breach log.

9. Evaluation and response

Once the initial incident is contained, a full review will be carried out examining the causes of the breach, the effectiveness of the response and whether any changes to systems, policies or procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how the personal data is held and where it is stored.
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure, sharing minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

BIOMETRIC DATA POLICY

1. Introduction

Monkseaton High School is committed to protecting the personal data of all its students and staff, this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

This policy outlines the procedure the school follows when collecting and processing biometric data.

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges

Biometric Data under GDPR is classified as special category data. Special Category data is Personal data which the GDPR says is more sensitive, and so needs more protection where biometric data is used for identification purposes, it is considered special category data.

2. Definitions

Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

Automated biometric recognition system: A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

Processing biometric data: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording students' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner / measurements of the face on a facial recognition scanner.
- Storing students' biometric information on a database.
- Using students' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise students.

3. Data protection principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

The school ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As the data controller, the school is responsible for being able to demonstrate its compliance

4. Data protection impact assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

The DPO will review the DPIA, once completed by the lead staff member.

The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

Where the school uses students' biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to receive school dinners instead of paying with cash or entry into the school site), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing a student's biometric data, the school will notify both parents/carers and students and written consent

will be sought from at least one parent/carer of the student before the school collects or uses a student's biometric data.

Notification sent to parents/carers will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used
- The parent's / carer's and the student's right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed

The school will not process the biometric data of a student under the age of 18 in the following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- No parent or carer has consented to the processing.
- A parent / carer has objected in writing to such processing, even if another parent has given written consent.

Parents/carers and students can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent(s) / carer(s).

Students will be informed that they can object or refuse to allow their biometric data to be collected and used.

Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s).

5. Alternative arrangements

Parents / carers, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

Where an individual object's to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service. For example, where the biometric system uses facial recognition to record school meals purchased, the student can use their name to record their meals.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the student's parents /carers, where relevant).

6. Data retention

Biometric data will be managed and retained in line with the IRSM Toolkit.

If an individual (or a student's parent / carer) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the school's system.

7. Breaches

There are appropriate and robust security measures in place to protect the biometric data held by the school.

Any breach to the school's biometric system(s) will be dealt with in accordance with the Data Protection Policy.

8. Monitoring and review

This policy will be reviewed on a 2 yearly basis.

Equality Impact Assessment

1. Name of the change, strategy, project or policy:	Data Protection Policy
2. Name of person(s) completing this form:	Marie-Anne Dowson

3. Has the policy/practice been assessed to consider any potential impact on the equality groups? Yes

Where potential impact has been identified, please complete questions 5-9, if none is identified, please sign and proceed to question 10.

4. Equality Target Group (highlight):	**Negative impact – it could disadvantage**	**Reason**
Race **Religion/belief** **Disability** **Gender** **Gender Reassignment** **Sexual Orientation** **Age** **Pregnancy/Maternity** **Marriage & Civil Partnerships**	**No significant impact.**	

5.	**Yes**	**No**
Is the impact legal/lawful? Seek advice from your School link HR Advisor if necessary.	n/a	n/a
Is the impact intended?	n/a	n/a
Does this action/policy/procedure attempt to meet the aims of the public sector equality duty? (this should feed into your Single equality scheme & action plan)	Yes, No, or N/A	If yes, please provide details
Eliminate unlawful discrimination, harassment and victimisation	n/a	n/a
Advance equality of opportunity between different equality groups	n/a	n/a
Foster good relations between different equality groups	n/a	n/a

7. If you have identified any negative impact, have you identified any ways of avoiding or minimising it?

8. Is it possible to consider a different policy/strategy/action, which still achieves your aim, but avoids any negative impact on people?

9. In light of all the information detailed in this form; what practical actions would you take to reduce or remove any negative impact?

10.a) As a result of the assessment and consultation completed in Part A above, state whether there will need to be any changes made to the policy, project or planned action.

10.b) As a result of this assessment and consultation, does the school need to commission specific research on this issue or carry out monitoring/data collection?

A) No changes required.
B) No

11. Have you set up a monitoring/evaluation/review process to check the successful implementation of the policy, project or change? If yes please provide details below.	**Yes**			

3 yearly review