Halton Lodge Primary School

Data Protection Policy – including GDPR

Date of last review: March 2018

Presented and approved by governors: March 2018

Date of next review: March 2021

Data Protection Policy – inc GDPR

1. INTRODUCTION

1.1 Halton Lodge Primary School is required to process personal data regarding staff, pupils and their parents and guardians, and friends of the school; relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy. *Processing may include obtaining, recording, holding, handling, disclosing, transportation, destroying or otherwise using data.*

In this Policy any reference to pupils, parents, friends or staff includes current, past or prospective pupils, parents, friends or staff.

1.2 All staff are responsible for complying with this policy.

2. SCOPE

2.1 This Policy covers the school's acquisition, handling and disposal of the personal and sensitive personal data it holds on all staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to governors and contractors. It explains the school's general approach to data protection, which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the school complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which become law on 25thMay 2018.

3. DEFINITIONS

3.1 Personal data:

The GDPR applies to 'personal data' meaning ***any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier***.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.2 Sensitive personal data is:

Any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings. **The GDPR refers to sensitive personal data as "special categories of personal data".** The special categories specifically include genetic data and biometric data, where processed, to uniquely identify an individual.

The school has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

a) Explicit consent of the data subject must be obtained;

b) Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement;

c) Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent;

d) Data manifestly made public by the data subject;

e) Various public interest situations as outlined in the General Data Protection Regulations 2018

3.3 The data subject is:

The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two pupils.

3.4 The Data Controller:

The school is the Data Controller and is responsible for determining the purposes of its use of data, what data it gathers, and how this information is used. As the Data Controller the school is responsible for complying with the Act.

3.5 The Data Protection Officer:

The school has appointed David Jones (Chair of Resources Committee) as its Data Protection Officer, responsible for day to day compliance with this Policy. He can be contacted via Halton Lodge Primary School by telephone (01928 564053) or email (head.haltonlodge@halton.gov.uk)

4. ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

4.1 The school shall only process personal data for specific and legitimate purposes.

These are:

a) providing pupils and staff with a safe and secure environment including images on CCTV – all cameras around the school carry appropriate warning signs as to their operation. They are used for the purpose of detecting crime, ensuring personal security and the welfare of staff and pupils and the protection of the working environment. Images are kept no longer than 28 days to meet these objectives. However, in certain circumstances - such as an on-going investigation into criminal activity - certain relevant images may be kept for longer; but no longer than necessary to complete any such investigation.
b) providing an education, training and pastoral care.
c) providing activities for pupils and parents - this includes school trips and activity clubs.
d) providing academic, examination and career references for pupils and staff.
e) protecting and promoting the interests and objectives of the school – this includes fundraising.
f) safeguarding and promoting the welfare of pupils.
g) monitoring pupils' and staff's email communications, internet and telephone use; to ensure pupils and staff are following the School's IT Acceptable Use Policy.
h) promoting the school to prospective pupils and their parents.
i) communicating with parents and carers.
j) for personnel, administrative and management purposes. For example, to pay staff and to monitor their performance.
k) fulfilling the school's contractual and other legal obligations.

4.2 Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer's permission.

4.3 The school shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The school shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

4.4 The school shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

4.5 When the school acquires personal information that will be kept as personal data, the school shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

4.6 The school shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School's Document Retention Policy. **Staff should not delete records containing personal data without authorisation.**

4.7 The School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

5. INFORMATION AND EXPLANATION

5.1 Privacy Notice: Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement (See Appendix 1: Privacy Notice *How We Use Pupil Information* and Appendix 2: *Work Force Privacy Notice*).

5.2 Purpose: The privacy notice is to ensure that the school's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with, how long records will be retained for and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

5.3 Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided. Copies of the Halton Lodge Primary School's privacy notice for pupils and parents can be obtained from the Data Protection Officer or accessed on the school's website.

5.4 Use: Having said this, staff should inform the Data Protection Officer if they suspect that the school is using personal data in a way which might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the school is collecting medical information about pupils without telling their parents what that information will be used for.

6. PROTECTING CONFIDENTIALITY

6.1 Disclosing personal data within the school: Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the school or their relationship to the data subject, unless they need to know it for a legitimate purpose. *For example, personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number*

and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

6.2 Disclosing personal data outside of the school: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

6.3 Before sharing personal data outside the school, particularly in response to telephone requests for personal data staff should:

a) make sure they are allowed to share it – that they have the necessary consent;
b) ensure adequate security. *What is adequate will depend on the nature of the data. For example, if the school is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; paper information should be sent by courier or recorded delivery, First or Second Class post is not considered secure enough;* and
c) make sure that the sharing is covered in the privacy notice.

6.4 The school should be careful when using photographs, videos or other media as this is covered by the Act as well. Specific guidance on this is provided in Appendix 3.

6.5 Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches.

Halton Lodge Primary School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the school shall take appropriate steps to prevent these events happening. In particular:

a) paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.
b) the school uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.
c) staff must not remove personal data from the school's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Data Protection Officer.
d) staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

7. DATA BREACHES

7.1 Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

7.2 Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as the school becomes aware of a significant data breach, as determined by the Data Protection Officer, it has 72 hours in which to report the breach to the Information Commissioner's Office.

Examples of breaches and their seriousness for reporting purposes are:

a) mistakenly sending an email or letter containing personal data to an incorrect recipient.
b) theft of IT equipment containing personal data.
c) failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious - i.e. if not dealt with, it is likely to result in a high risk to the rights and freedoms of individuals (e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage) then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer.

8. DATA SUBJECT'S RIGHTS, INCLUDING ACCESSING ANY DATA HELD ON THEM

8.1 Individuals are entitled to know whether the school is holding any personal data which relates to them, what that information is, the source of the information, how the school uses it and who it has been disclosed to. **This is known as a Subject Access Request.**

Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer.

Any member of staff who receives a request for information covered by this policy from a pupil, parent or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. <u>This is important as there is a statutory procedure and timetable which the school must follow</u>. Information must be provided to the requestor without delay and at the latest within one month of receipt.

8.2 Individuals have a right to ask the school not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

8.3 Individuals have a right to ask for incorrect personal data to be corrected or annotated.

8.4 Individuals have the right to object to any of their personal data being processed and to have this data erased.

8.5 Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

8.6 Individuals have the right to request their personal data is transferred to another data controller in a commonly used format.

8.7 Individuals have a right to ask the school not to make automatic decisions (using personal data) if such automatic decisions would affect them to a significant degree.

8.8 Individuals have the right to complain about the processing of their personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

9. DATA PROCESSORS

9.1 Where the school uses data processors (third parties / organisations that process (deals with or stores) personal data on the school's behalf, the GDPR makes written contracts between the school and the processor a general requirement and that the contract must include certain specific terms as a minimum. **If the data processor then (with the school's written authority) employs another processor, it also needs to have a written contract in place.**

The school will check all existing contracts and if they do not contain all the requirements it will get new contracts drafted and signed as required.

The school will ensure data processors are communicated with so they understand:

- the reasons for the changes;
- the new obligations that GDPR put on them; and
- that they may be subject to administrative fines or other sanctions if they do not comply with new obligations.

New and existing contracts must comply with GDPR by 25th May 2018.

10. RECORDS MANAGEMENT AND RETENTION

10.1 Section 46 of the Freedom of Information Act 2000 requires schools to follow a Code of Practice on managing their records. Under section 7 of the Code of Practice on the Management of Records, it states that:
'Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy.'

10.2 The school recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This section of the Data Protection Policy provides the framework through which this effective management can be achieved and audited.

10.3 Scope of the policy - This policy applies to all records created, received or maintained by staff of the school in the course of varying out its functions.

10.4 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

10.5 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the Cheshire County Archives Service.

10.6 Responsibilities - The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher.

10.7 The Headteacher will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely. They will also liaise with the Local Authority, when appropriate.

10.8 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

10.9 Documents having reached their scheduled destruction age must be cross checked with any litigation or complaints procedures or ombudsman or OFSTED etc. and if any of these apply the documents should not be destroyed.

10.10 The school will make reference to the Records Management Society of Great Britain's Retention Guidelines for Schools. (This retention schedule contains recommended periods for the different record series created and maintained by schools in the course of their business).

11.FURTHER INFORMATION

11.1 The school has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the school's register entry on the Information Commissioner's website at **www.ico.gov.uk** under registration number Z531318X. This website also contains further information about data protection.

12. BREACH OF THIS POLICY

12.1 A member of staff who deliberately or recklessly discloses personal data held by the school without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

13. PROCEDURES FOR ACCESS TO PERSONAL INFORMATION (SUBJECT ACCESS REQUESTS)

13.1 Rights of access to information - There are two distinct rights of access to information held by schools about pupils. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing:

> Under the Data Protection Act 1998 / GDPR 2018, a pupil has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see below).
>
> The right of parents to have access to curricular and educational records relating to their child as defined within the Education (Pupil Information) (England) Regulations 2005.

13.2 Dealing with a request - These procedures relate to the above mentioned rights.

13.3 Requests for personal information must be made in writing and addressed to the Headteacher**.** *If the initial request does not clearly identify the information required, then further enquiries will be made.*

13.4 The identity of the requestor must be established before the disclosure of any personal information, and checks should also be carried out regarding proof of relationship to the child.

13.5 Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

13.6 Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand. *As a general rule, a child of 13 or older is expected to be mature enough to*

understand the request they are making. If the child cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf.

13.7 The Headteacher should discuss the request with the child and take their views into account when making a decision.

13.8 The school must provide a copy of the information **free of charge**. However, the school can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. *The school may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean the school can charge for all subsequent access requests. The fee will be based on the administrative cost of providing the information.*

13.9 The response time for subject access requests, once officially received, is **a calendar month.**

13.10 There are some exemptions to the right to subject access that apply in certain circumstances or to certain types of personal information. Therefore, all information must be reviewed prior to disclosure.

13.11 Responding to a request may involve providing information relating to another individual (a third party). Third party information is that which identifies another pupil/parent or has been provided by another agency, such as the Police, Local Authority, Health Care professional or another school. *Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the calendar month timescale.*

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

13.12 If there are concerns over the disclosure of information then additional advice should be sought from the school's Data Protection Officer.

13.13 Where redaction (information edited/removed) – see Appendix 4 - has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

13.14 Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

13.15 Information can be viewed at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.

13.16 The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

13.17 Complaints - Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

13.18 Contacts - If you have any queries or concerns regarding access to records or the Data Protection Act, then please contact the school's Data Protection Officer.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

14. STATUS

14.1 This policy is intended only as a statement of School policy. It does not form part of the contract of employment and may be amended from time to time.

15. RELATED POLICIES:

Privacy Notice for Pupils and Parents – Appendix 1
Privacy Notice for Staff - Appendix 2
A Guide To Press and Publicity in Primary Schools & Use of Recording Equipment – Appendix 3
Redaction Procedure – Appendix 4
Information Security Guidance For Schools – Appendix 5
Disposal of Redundant ICT
Staff Behaviour and Conduct Policy
Staff Acceptable Use Policy Agreement

16. FURTHER INFORMATION

16.1 Further information and guidance regarding this policy or its application can be obtained from the Data Protection Officer.

This policy has been developed using all of the model policies relating to GDPR produced by Halton Borough Council (Peter Richmond) in December 2017, January 2018 and February 2018.

Appendix 1:

Halton Lodge Primary School
Privacy Notice: How We Use Pupil Information

Why do we collect and use pupil information?

We collect and use pupil information under the General Data Protection Regulations (GDPR):

Article 6 - Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law, and

Article 9 - Processing is necessary for reasons of substantial public interest, on the basis of law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The GDPR comes into force on 25th May 2018

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing.

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

- Personal information (such as name, unique pupil number, address, contact details and previous school/nursey attended);
- 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 (such as termly assessment data, reading levels and attainment in end of key stage tests);
- Relevant medical information (such as allergies and long-term medical conditions);
- Special education needs information (such as area of need and level of support required);
- Exclusions and behavioural information (such as reasons for exclusions, cause for concern records and serious incident logs).

Collecting pupil information

Whilst the majority of pupil 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 pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for seven years after the child leaves the school – unless this needs to be retained for another purpose.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupils attend after leaving us;
- our local authority;
- the Department for Education (DfE);
- Halton Children's Safeguarding Board;
- School nurse (and NHS);
- Cheshire police.

Why we share pupil information

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

We share pupils' 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 pupils 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.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils 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 pupils 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 pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

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 pupils 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 pupil 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 pupil 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 pupils 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 the Headteacher (See CONTACTS section below).

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, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF. Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

Contacts:

If you would like to discuss anything in this privacy notice, please contact:

Anthony Hilldrup (Headteacher)
Halton Lodge Primary School, Grangeway, Runcorn, WA7 5LU.
Tel: 01928 564053
Email: head.haltonlodge@halton.gov.uk

If you need information about how the Halton Borough Council and DfE store and use your information, then please go to the following websites:

http://www4.halton.gov.uk/Pages/Home.aspx
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you cannot access these websites, please contact Halton Borough Council or the DfE as follows:

Janet Johnson – Information Governance – ICT Services – Halton Borough Council
Direct Dial Tel: 0151 511 7059 or via email janet.johnson@halton.gov.uk

DfE - Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
Website: https://www.gov.uk/government/organisations/department-for-education
Email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Peter Richmond (Divisional Manager - Service Improvement / Governance)
Resources & ICT Services, Halton Borough Council, Municipal Building, Kingsway, Widnes, WA8 7QF
Email: peter.richmond@halton.gov.uk (for person identifiable data please use peter.richmond@halton.gcsx.gov.uk)
Direct line: 0151 511 7003 Switchboard: 0303 333 4300

Appendix 2

Halton Lodge Primary School
Work Force Privacy Notice

We, Halton Lodge Primary School are a Data Controller for the purposes of the 2018 Data General Data Protection Regulations (GDPR) and previously the Data Protection Act of 1998.

Personal data is held by the school for those employed or otherwise engaged to work at the school or Local Authority. This is to assist in the smooth running of the school and/or enable individuals to be paid.

How we use school workforce information

The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed
- Informing the development of recruitment and retention policies;
- Allowing better financial modelling and planning;
- Enabling ethnicity and disability monitoring;
- Supporting the work of the School Teacher Review Body;
- Support Staff Negotiating Body.

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

- personal information (such as name, 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).

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 GDPR articles:

6 (c) processing is necessary for compliance with a legal obligation to which the controller is subject;

6 (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

9 (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

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 GDPR 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 seven years after the termination of employment.

Who we share this information with

We routinely share this information with:

- our local authority (Halton)
- the Department for Education (DfE)
- Disclosure and Barring Service.

Under the General Data Protection Regulation (2016/679 EU) (GDPR), personal data relating to criminal convictions and offences can be processed only:

under the control of official authority; or

when it is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

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 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 the headteacher
Anthony Hilldrup, Halton Lodge Primary School, Grangeway, Runcorn, WA7 5LU. 01928 564053.

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:

Anthony Hilldrup (Headteacher)
Halton Lodge Primary School, Grangeway, Runcorn, WA7 5LU.
Tel: 01928 564053
Email: head.haltonlodge@halton.gov.uk

Appendix 3:

A Guide To Press and Publicity in Primary Schools & Use of Recording Equipment

1. **Background -** There is increasing concern over the use of photography and video in schools where this is not carried out by the school. E.g. the press, parents etc.
   Some schools have banned parents from videoing school events for fear of the recordings being used by paedophiles or by estranged family members when there are child protection concerns. Similarly the printing of pupil's names in press reports or photographs has led to concern over child protection issues and confidentiality.

   The purpose of this guidance is to offer Headteachers and the governing body advice on this matter, although it is ultimately a local decision which should be made by Headteachers in consultation with governing bodies and parents.

2. **Recommended Good Practice -** The Data Protection Act / GDPR is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with pleasure.

   Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

   - Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.
   - Photos taken purely for personal use are exempt from the act.

3. **Printing of Pupil Names by the Press -** Many schools encourage and welcome the press in school to report on special events and particular successes. This is an important vehicle for raising the profile of the school in the local community and celebrating achievement both for the school and individual pupils.

   Sometimes the press arrives uninvited if they sense a 'good story' for whatever reason.

   In the past if a photograph is printed it has been accepted practice for the caption to include full names and ages of the pupils. In some cases, the newspaper is reluctant to print unless this information is provided.

   In order to protect the identity of the minority of children where this could be a problem or a concern to parents the following advice is offered.

a) Provide only first names and ages. *If it is appropriate or reasonable obtain prior permission from parents/carers to use full names. (eg of individual or small number of children when the press visit is known well in advance).Only allow full names to be printed if <u>all</u> parents/carers of the subjects agree to*

this.

b) Only allow interviews if parent/carer permission has been obtained in advance and they are aware of the reason for and content of the interview.

4. Television and Radio - Always seek parent/carer permission in advance before pupils are interviewed for radio and television. Ensure they are fully aware of the purpose and content of the interview.

5. Photography and Videoing in School

5.1 **By Parents/carers -** Parents/carers are understandably keen to record their children's special moments in school such as appearances in school productions, sports days etc. It is up to the school to decide whether the use of video equipment is appropriate on a case by case basis as this can be quite intrusive and spoil others enjoyment of the event.

If it is decided that parents / carers are to be allowed to photograph or video, schools may wish to ask parents to sign an undertaking that any resulting photographs or video is for personal use only and will not be sold or used for any other purpose.

5.2 **By the School -** Photographs and/or videos are regularly taken in school to provide a record of special events or simply for teaching purposes. Sometimes videos or photographs are sold to parents who wish to have their own copies. E.g. of music or drama productions, photographs of schools trips.

When this is done it is good practice to obtain parental permission in advance particularly if copies are to be on sale afterwards.

If photographs of pupils or students are taken for building passes, these images are likely to be stored electronically with other personal data and the terms of the Act will apply.

6 General Advice

- Agree the guidance within your local cluster group or area so that there is consistency for:
    a) Parents; and
    b) Any local paper which covers your area, who will know what to expect.
- Initiate a discussion at your annual parents meeting to sample the views of parents;
- Obtain approval from your governing body for the school's policy;
- Publish a short statement in the school prospectus or brochure reflecting the school's policy;
- Make it clear that it is the parent /carer responsibility to inform the school if the identity of any child at the school should not be disclosed at all. Ask for legal confirmation of this for file; (eg copy of an injunction)
- If appropriate, design a simple disclaimer / permission slip for parents to sign giving permission for:
    a) full names to be provided to the press, and
    b) photography or videoing to be carried out.

Consider sending your local paper a copy of the policy agreed by your local cluster or area.

Appendix 4:

Redaction Procedure

1. Introduction

1.1. This procedure is based on The National Archives Redaction Toolkit which provides a guide to editing exempt information from paper and electronic documents prior to release.

1.2. This procedure should work in conjunction with any team/departmental guidance. If there is any contradiction between the two, please consult the Information Governance Team for advice.

2. What is redaction?

2.1. Redaction is the separation of disclosable from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of the document. In the paper environment some organisations will know redaction as *extracts* when whole pages are removed, or *deletions* where only a section of text is affected.

3. Principles of redaction

3.1. Always carry out redaction on a copy of the original record, whether paper or electronic, never on the record itself. This ensures that while the redacted information is permanently removed from the copy of the record (which can then be made accessible) the original text remains in the original record. Redaction should never result in the complete removal of text or information from an original record.

3.2. Redaction is carried out in order to edit exempt details from a document. Use it when one or two individual words, a sentence or paragraph, a name, address or signature needs to be removed.

3.3. If so much information has to be withheld that a document becomes meaningless, the entire document should be withheld. In the case of paper documents the same principle should apply to individual pages.

3.4. Redaction should be performed or overseen by staff that are knowledgeable about the records and can determine what material is exempt. If those identifying such material do not carry out the redaction themselves, their instructions must be specific - so for example: 'Memo dated …, paragraph no…, line starting… and ending…' and so on.

3.5. Under FOI, applicants may request information presented in electronic form. For paper documents, this will usually mean scanning the redacted version of the material. If, however, the level of resources required to do the scanning would make this unduly onerous, the FOIA allows the organisation to set aside the applicant's stated preference on the grounds of practicability (Section 11).

4. Identifying material for redaction

4.1. To comply fully with requests for information, redact exempt material only. A whole sentence or paragraph should not be removed if only one or two words are non-disclosable, unless release would place the missing words in context and make their content or meaning clear.

4.2. In the case of electronic records close examination of the internal bit stream of the file can reveal the length of the redacted content. Take great care to ensure that the non-disclosable material cannot be deduced. This may mean disguising the size and shape of the redacted content. This is especially the case where the non-disclosable information appears in several locations within the file, and where there is an increased chance of deciphering such redacted content using a combination of location pattern, bit length and the associated unredacted text.

4.3. Reviewers should consider that earlier statements in a document might suggest the content of removed material. For example, if a paragraph refers to reports from overt sources, and the following paragraph refers to reports from covert sources, as well as removing the words 'covert sources', 'overt sources' would also need to be removed or the meaning of the missing words from the second paragraph could be inferred.

5. Keeping records of redaction work

5.1. Once reviewers have identified redactions, agreed with any other interested parties, decisions need to be recorded. This can either be by keeping a copy of the released version of the documentation, with a note explaining the reasons for redaction, or keeping a detailed list of the redacted information. This will then be retained in line with the Retention Schedule.

6. Redaction of documents

6.1. Always carry out redaction on a copy, leaving all the information contained in the original document intact.

6.2. There are a range of redaction methods (see Section 7), and any may be used effectively according to issues such as the structure and content of the document, the degree of confidentiality, and the cost and time available.

6.3. Whichever method is used, the end result must ensure that the redacted material cannot be seen or guessed due to incomplete redaction. This means checking to make certain that words cannot be made out when the document is held up to light or that the ends, top or bottom of text are not visible.

6.4. Every document that is redacted should be checked by a secondary party to verify that there is nothing further that requires redacting which has been missed.

7. Methods of redaction

7.1. **Cover-up tape** – The simplest form of redaction is to use a high quality cover-up tape that can be placed on the original documents over the areas to be redacted, taking care that no parts of words

are showing. By making a photocopy of the redacted text, an access version is produced ready for presentation.

7.2. **Blacking/whiting out** – Another simple solution is to photocopy the original document and use a black marker pen to block out the sensitive material. The redacted version should then be photocopied again to produce an access version. The further photocopy is necessary as information redacted using marker pen can be read when held up to light.

7.3. **Correction fluid** – The same process can be used substituting a good quality correction fluid for marker pen. Ensure that no redacted text is visible before making the second photocopy, which again is necessary as correction fluid can be easily removed.

7.4. **Electronic records** – These can be printed as a hardcopy and redacted as above or the information may be redacted from an electronic copy, which is then printed. If the redacted copy is required in electronic format, this can be created by scanning the redacted paper copy into an appropriate format, such as Adobe Portable Document Format.

7.5. This approach is currently recommended by The National Archives, if it meets the business requirements of the organisation.

8. Redaction Guidance

8.1. **Consent** – Where consent is given or could reasonably be expected to be given then third party information does not need to be redacted. **The decision whether it is appropriate to do so should be made on a case-by-case basis**. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. You must not apply a blanket policy of withholding it.

8.2. **Information generally known by the individual making the request** – If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public; it will be more likely to be reasonable for you to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual.

8.3. **Circumstances relating to the individual making the request** – The importance of the information to the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life. Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent.

8.4. **Social work, health and educational records** – Special rules govern subject access to social work, health and educational records. In practice, these rules mean that relevant information about social work, health or education professionals (acting in their professional capacities) should usually be disclosed in response to a SAR.

Social Care – Special rules apply where providing subject access to information about social care and related activities which would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the requester or any other person. These rules are set out in the Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI 2000/415). Their effect is to exempt personal data processed for these purposes from subject access. To apply this exemption, there clearly needs to be an assessment of the likelihood of the disclosure causing serious harm. If you are not a social care professional, you must consult the social care professional who is responsible for the care of the individual concerned before deciding whether the exemption applies. A further exemption from subject access to social work records applies when a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party. The decision regarding redaction in this situation should only be made by a qualified social work professional.

Health – Special rules apply where providing subject access to information about an individual's physical or mental health or condition would be likely to cause serious harm to them or to another person's physical or mental health or condition. These rules are set out in the Data Protection (Subject Access Modification) (Health) Order 2000 (SI 2000/413), and their effect is to exempt personal data of this type from subject access to the extent that its disclosure would be likely to cause such harm. To apply this exemption, there clearly needs to be an assessment of the likelihood of the disclosure causing serious harm. If you are not a health professional, you must consult the health professional who is responsible for the clinical care of the individual concerned before deciding whether the exemption applies. This requirement to consult does not apply if the individual has already seen or knows about the information concerned. A further exemption from subject access to information about an individual's physical or mental health applies where a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party.

Education – In deciding what information to supply in response to a SAR, you need to have regard to the general principles about exemptions from subject access described elsewhere in this document. Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

- Information that might cause serious harm to the physical or mental health of the pupil 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; and
- Certain information given to a court in proceedings concerning the child.

9. The Information Commissioner's Office

9.1. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Complaints relating to Data Protection and Freedom of Information can be escalated to the ICO.

9.2. Failure to redact documentation correctly is a breach of the Data Protection Act and could lead to sanction from the ICO. The ICO has the power to fine authorities up to £500,000 for serious breaches.

10. Data Protection

10.1. The Data Protection Act 1998 places a legal obligation on all organisations to process personal data in accordance with eight Data Protection Principles set out in the Act. The Act gives enforceable rights to individuals (data subjects) and places obligations on those legal persons who control the manner and the purpose of the processing of personal data (data controllers).

11. Supporting Guidance

11.1 The ICO guidance on 'How to disclose information safely' goes into more detail when disclosing information which has been derived from personal data and requires further processing to ensure that individuals cannot be identified from that information. This is relevant when dealing with FOIs, SARs or Environmental Information Requests. ICO's website www.ico.org.uk

Appendix 5:

Information Security Guidance for Schools

The Data Protection Act 1998 is a law that protects personal privacy and upholds an individual's rights. Central to the Act are the eight data protection principles. The seventh principle of the Act refers to appropriate security measures being taken to protect unauthorised or illegal processing.
All personal data whether manual or electronic must be kept secure to prevent accidental loss, damage or destruction. The extent of the security measures required will depend on the sensitivity of the data.
Here are some basic Dos and Don'ts:

- Lock the office when leaving it unattended for any length of time to prevent unauthorised access to personal information.
- Manual records containing personal information should be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding or use the confidential waste bins.
- Do not share your user ID or password with anyone.
- If you have a laptop which holds personal data, make sure it is encrypted.
- Ensure that your computer screen cannot be viewed by any unauthorised personnel.
- Do not send personal information by fax unless the information has been de-personalised or the fax machine is a 'safe haven' one (in a secure area, which is locked when unattended).
- Do not send personal information by unsecured email as its security cannot be guaranteed. If it is necessary to send information in this way and you do not have access to secure email, make sure the personal information has been either password protected or de-personalised. Send the data as an attachment to the email and flag as confidential.
- If sending any email to multiple recipients outside of the school, consider using blind copy facility so recipients can't view other recipients' email addresses (which, depending on the subject of the email, could constitute personal information)
- If you are required within the course of your duties to take personal data home (including laptops, videos, etc.), do not leave the information unattended for any length of time, especially in a vehicle overnight.
- Do not give out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the caller's name and switchboard telephone number and verify their details before responding.
- Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.
- Remember - at all times treat people's personal information as you would wish your own to be treated.

Transporting information Securely

When there is a need to transport information held within documents, laptops, mobile devices etc., which are of a confidential nature i.e. personal to staff or pupils, or commercially sensitive, it is important to ensure precautions are taken to reduce the possibility of these being stolen.

This is also a requirement of Principle 7 of the Data Protection Act 1998, which requires data to be kept safe and secure, ensuring that information cannot be accessed by unauthorised persons.

Employees should therefore take all reasonable steps to ensure security is maintained when transporting information between work and home or between work-bases.

Documents and mobile devices should be transported in a way to minimise the opportunity of destruction or loss by ensuring vehicles used to transport them are kept locked and secure particularly when unoccupied.

Car Crime

Many thefts from cars are opportunist crimes of items that may or may not be of value, but are visible to a thief. Thefts can occur whilst stationary at traffic lights, moving through slow moving traffic or whilst parked in a drive/car park. They do not necessarily have to occur when vehicles are left unattended in badly lit or deserted places.

Opportunist thefts take place anywhere, anytime and often within seconds.

Good Practice

- The best guard against theft of personal information and mobile devices is to avoid having to transport where there is no absolute need.
- Avoid transporting complete files. Only take the relevant documents where possible.
- Do not advertise that you are or will be taking home or transporting items of a confidential nature.
- Ensure that personal information or mobile devices are transported within secure bags, boxes, folders etc to reduce the risk of loss or damage.
- Personal information and mobile devices transported in vehicles should be kept hidden away in a locked boot wherever possible or otherwise kept out of sight to discourage opportunist grab crimes.
- Personal information and mobile devices should not be left unattended even in locked vehicles especially overnight.
- If you can, take personal information or mobile devices with you when you leave your vehicle.
- Aim to park in busy, well-lit areas or where there is CCTV coverage to discourage thieves.
- If leaving your vehicle even for a second, whilst paying for petrol, using a cashpoint or just popping into a newsagents, ensure your vehicle is secure and that doors, windows, the boot and sunroof are all locked.

Sharing Information Securely

By Post

If you are sending personal information by post, you must:

- confirm the name, department and address of the recipient;
- seal the information in a robust envelope;
- mark the envelope 'Private and Confidential – To be opened by Addressee Only' and place this inside a larger envelope with only the correct name and address on it - this adds an additional level of security as the package is not easily identifiable as 'valuable' and administrative staff should only open the outer envelope;

If you are sending sensitive personal information by post, you must also:

- send the information by recorded, registered or 'signed for' delivery or by courier where appropriate;
- ask the recipient to confirm receipt; and
- record the disclosure on the service users file
- Registered post is the best way to send sensitive personal or confidential information on an encrypted CD.

Different levels of security can be used depending on the information being sent:

- Reliable transport couriers should be used at all times. Consult with your organisation.
- Packaging must be adequate to protect the contents from damage during transit.

By Telephone

If you have received a request to share personal information via the telephone, you must first confirm that the requestor is who they say they are and has a legitimate reason for access to the information.
Where possible ask for the request to be put in writing or if urgent ask for their contact details. Only accept the main switchboard number of their organisation and confirm with the operator the name, job title, department and organisation of the person with whom you wish to share information. Do not accept a mobile phone number.

Once you have confirmed this:

- do not share information when a return telephone number cannot be supplied - call the practitioner back via the switchboard;
- only provide the information to the person who has requested it - if they are not there you should leave a message for them to call you back;
- do not leave a detailed (disclosure) message with someone else or on a voicemail;
- be aware of who might overhear your call;
- keep a record of any personal information disclosed during the call; and
- record on the service users file the time of the disclosure, the reason for it and if appropriate, who authorised it.

By Fax

Paper documents are often sent by fax. Precautions must be taken when sending personal information by fax because the receiving machine may be sited in an open office, meaning the document is visible to other staff, contractors or visitors. Where possible any information should be shared via a dedicated fax (known as a 'safe haven' fax machine).

If you are sending information by fax to a machine that is NOT a safe haven one you must:

- remove any information that could identify an individual
- telephone the recipient of the fax to let them know you are about to send it;
- check the fax number. If the information is confidential ask them to wait by the fax;
- ask the recipient to confirm receipt of the fax; or call them to ensure the fax has arrived;
- use pre-programmed fax numbers where possible to reduce the chance of the fax being sent to the wrong machine;
- ensure that you use an appropriate fax cover sheet. Make sure your cover sheet states who the information is for, and mark it 'Private and Confidential';
- ensure you do not refer to the names of the person(s) concerned in the subject heading or on the cover sheet of the fax;
- keep a record that you have sent the fax on the service users file.

By email

Huge amounts of information are sent by email, within and across agencies. Whilst internal messages are generally secure (e.g. within organisations), those sent to external addresses are not considered secure enough for personal information. Personal information must be sent by other methods, some of which are outlined in this section.

When sending personal information via email, you should:

- ensure all recipients need to receive the information - think twice before responding to a group email or copying others in;
- confirm the name, department and email address of the recipient;
- use a flag to mark the message 'confidential';
- do not include personal or confidential information in the subject field;
- ask the recipient to confirm receipt of the email;
- If sending any email to multiple recipients, consider using blind copy facility so recipients can't view other recipients' email addresses (which, depending on the subject of the email, could constitute personal information)

Using password protected files

Password protection and encryption are not necessary for information shared between staff within a secure platform (e.g. within the school) or where secure email is used.

- If you have to send personal information to an external recipient, contain it within a password protected file.

- Remember to use a different password to anything you may use for other tasks because you will have to share the password when you disclose the document.
- Always save the password protected version of the document as a new file and retain the original safely. IT Services will not be able to open password protected or encrypted documents without the password.
- Do not send the password in the same email - preferably ask the recipient to confirm receipt of the information and then send the password in the reply to that email. Or give the password over the telephone.
- Record what information has been sent on the service users file.
- After receiving a password protected file, re-save the information without the password in a new secure place. Do not rely on remembering the password.
- Save an audit trail of your email communications. This could mean saving a copy of all sent and received emails in a separate folder.

Sending information by Secure Mail

When sharing information with other organisations there are some secure methods available, for example the S2S system.

The S2S system allows schools and local authorities to securely share information, for example to:

- transfer pupil records using the common transfer file protocol (CTF)
- update pupil details with the Learning Records Service (LRS)
- apply for and receive pupil unique learning numbers
- send and receive messages to and from other users within the S2S network.

To send information to another school or local authority, you must:

- use the CTF naming protocols
- save the data in an encrypted folder or file
- send the file as a compressed folder

Full instructions for saving, uploading and receiving files via S2S can be found in the guides for schools and local authorities.

In Person

- Personal or confidential information may be delivered personally by members of staff. Such information may be held in paper or electronic form. Where laptops, PDAs or other electronic devices are used precautions must be taken to ensure the security of systems as well as any data held on the device itself.
- Personal information should only be taken off site where necessary, either in accordance with local policy or with the agreement of your line manager.
- Log any personal information you are taking off site and the reason why.
- Paper based personal information must be transported in a lockable box, sealed file or envelope.

- Electronic information must be protected by appropriate electronic security measures – password or encryption.
- If transferring personal information by car put the information in the boot and lock it, but DO NOT leave in the car overnight
- Ensure the information is returned back on site as soon as possible.
- Record that the information has been returned.

Cloud Computing

Cloud computing is defined as access to computing resources, on demand, via a network. By processing information in the cloud an organisation may encounter risks to data protection that they were previously unaware of. It is important that data controllers take time to understand the data protection risks that cloud computing presents.

Cloud computing is not a one-size-fits-all product and in many cases it can be tailored to fit the specific needs of an organisation. The compliance issues that arise will depend on the type of cloud service in question.

The processing of certain types of personal information could have a greater impact on individuals' privacy than the processing of others. With this in mind, the cloud customer should review the personal information it processes and determine whether there is any data that should not be put into the cloud. This may be because specific assurances were given when the personal information was collected. Often the question may not be whether the personal information should be put into the cloud but what the data protection risks are and whether those risks can be mitigated.

Here is a link to guidance issued by the ICO: -

http://ico.org.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

The guidance includes this checklist to consider:

Risks

- Make a list of the personal information you hold and how it will be processed in the cloud.

Confidentiality

- Can your cloud provider provide an appropriate third party security assessment?
- Does this comply with an appropriate industry code of practice or other quality standard?
- How quickly will the cloud provider react if a security vulnerability is identified in their product?
- What are the timescales and costs for creating, suspending and deleting accounts?
- Is all communication in transit encrypted? Is it appropriate to encrypt your information at rest? What key management is in place?

- What are the information deletion and retention timescales? Does this include end-of-life destruction?
- Will the cloud provider delete all of your information securely if you decide to withdraw from the cloud in the future?
- Find out if your information, or information about your cloud users will be shared with third parties or shared across other services the cloud provider may offer

Integrity

- What audit trails are in place so you can monitor who is accessing which information?
- Make sure that the cloud provider allows you to get a copy of your information, at your request, in a usable format.
- How quickly could the cloud provider restore your information (without alteration) from a back-up if it suffered a major data loss?

Availability

- Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers?
- How could the actions of other cloud customers or their cloud users impact on your quality of service?
- Can you guarantee that you will be able to access the information or services when you need them?
- How will you cover the hardware and connection costs of cloud users accessing the cloud service when away from the office?
- If there was a major outage at the cloud provider how would this impact on your business?

Legality

- Make sure you have a written contract in place with your cloud provider.
- How will the cloud provider communicate changes to the cloud service which may impact on your agreement?
- Which countries will your cloud provider process your information in and what information is available relating to the safeguards in place at these locations? Can you ensure the rights and freedoms of the data subjects are protected?
- You should ask your cloud provider about the circumstances in which your information may be transferred to other countries.
- Can your cloud provider limit the transfer of your information to countries that you consider appropriate?

Information Security Breaches

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

The Information Commissioners Office (ICO) has the power to issue monetary penalty notices. Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

If despite the security measures you take to protect the personal information you hold a breach of security occurs, it is important that you deal with the security breach effectively. The breach may arise from a theft, a deliberate attack on your systems, from the unauthorised use of personal information by a member of staff, or from accidental loss or equipment failure. However, if a breach occurs, you must respond to and manage the incident appropriately.

Having a policy on dealing with information security breaches (see Data Protection Policy) is another example of an organisational security measure you may have to take to comply with the seventh data protection principle.

There are four important elements to any breach-management plan:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.

4. Evaluation and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly.

Reporting a breach

Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as the School becomes aware of a significant data breach as determined by the Data Protection Officer it has 72 hours in which to report the breach to the Information Commissioner's Office. Examples of breaches and their seriousness for reporting purposes are:

a) mistakenly sending an email or letter containing personal data to an incorrect recipient.
b) theft of IT equipment containing personal data.
c) failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer.

Appendix 6:

Disposal of Redundant ICT Equipment

All redundant ICT equipment should be disposed of through an authorised agency or via the Halton Borough Council disposal scheme. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

If ICT equipment is to be disposed of via the Council's disposal scheme, details MUST be entered via the **IWantIT** portal selecting the Asset Disposal option and filling in all of the required details or emailed to the Halton Borough Council Schools manager. ICT Services will then arrange to have the equipment collected from the school and ensure that all asset information is passed back to the school. It is the responsibility of the school to ensure that any data that is of a confidential or personal nature is removed.

All redundant ICT equipment that may have held personal data must have the storage media over written multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

The school's disposal record will include:

- Date item disposed of;
- Authorisation for disposal, including verification of software licensing and any personal data likely to be held on the storage media;*

* *If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.*

- How it was disposed of e.g. waste, gift, sale;
- Name of person and/or organisation who received the disposed item.

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate. All software and data relating to the school should have been removed and the hardware reset to factory default.

Further information is available from:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx