Data Protection Impact Assessment – School Data Usage

Introduction

Article 35 of the General Data Protection Regulation 2016 as enacted in UK law by the Data Protection Act 2018 requires that a Data Protection Impact Assessment is carried out where there is a likelihood of "high risk to the rights and freedoms of natural persons" [Article 35 (1)].

Schools processing is considered unlikely to be classified as having such high risk, however we have carried out this assessment in order to ensure that we are fully compliant.

Each of the following sections provides the requisite portions of the Article 35 (7) requirements for a Data Protection Impact Assessment. Note that as part of data governance improvements the school is, with the Local Authority, carrying out further work in this area to provide risk assessment at the individual system level

Description of the envisaged processing operations

Data is used in the school in accordance with our published privacy statement. Specifically, we process data in order to:

- deliver education
- contact the right people about issues
- ensure a healthy, safe environment for learning
- carry out our functions as an employer

We are required to carry out the function of delivering education by the various laws including the Education Act, and all our data usage is consequential upon that requirement.

Processing of data about pupils has the following purposes:

- 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 about data sharing with other organisation (e.g. Department for Education)
- To support behaviour management and assessment
- To safeguard pupils
- To improve communication with parents

We additionally process data about people who are responsible for pupils for the following purposes:

- to contact them, both routinely and in emergencies
- to ensure they are kept aware of pupil's progress as appropriate
- to comply with the law regarding data sharing

We also process data about our school's workforce:

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

Assessment of the necessity and proportionality of the processing operations in relation to the purposes

All data processing is designed to achieve the primary purposes noted above. No processing is carried out that is not required for the purposes, or assists in achieving the purposes.

Assessment of risks to rights and freedoms of data subjects

This, along with the assessment of security measures undertaken, is provided at appendix A

Measures envisaged to address the risks, Rights of Data Subjects

Our use of data is governed by the various acts relating to education and therefore the majority of data use is based on legal basis. We also have responsibilities for child protection, and these are covered by the Safeguarding regulations. Consent is only used for data items not covered by these legal areas – generally for optional activities such as clubs and school trips.

Data subject rights are always considered and how to access rights is published in our privacy statement.

Our measures to address risks are addressed by the Article 32(1) measures documented below:

(a) the pseudonymisation and encryption of personal data.

We use encryption where possible for data on end user devices; encryption is always used where electronic data is in transit outside of our school. We do not use pseudonymisation within the school.

Electronic data access by parents and pupils outside the schools takes place on their own equipment; we encrypt in transit, but it is not practicable to force encryption on these personal devices.

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Confidentiality – all systems have role-based access control and many are also restricted to access only from our school network. There are policy and discipline frameworks in place to provide further controls, and access is logged.

Integrity – we regularly review data on our systems, and they are subject to audit. There are also additional verification controls on some systems.

Availability / Resilience – there are service level agreements in place for cloud-based services. For on-site services we use methods such as replication of equipment (e.g. redundant power supplies, RAID) where necessary, and protection for power outages such as uninterruptable power supplies.

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

For cloud services this is dependent on the cloud supplier; we have contractual controls regarding backup and restore as required in these contracts. For on-site services we have regular backups which include testing of backups to ensure recoverability.

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Audits are carried out on our systems; backup testing is undertaken. Where risk warrants, external tests such as penetration testing are used.

May 2018

Appendix A – Assessment of Key Risks

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
	Risk Title	Identify the problem and list the relevant risks and the potential impact / consequence of each.	1=Rare 2=Unlikely 3=Possible 4=Likely 5=Almost certain	1=Insignificant, 2=Minor, 3=Moderate 4=Major, 5=Extreme (See Guidance For Scoring)	Likelihood x Impact (Red Amber Green)	What existing processes / mitigations are in place to manage the risk? Actual Controls.				What further mitigating actions (if deemed necessary) is planned to treat the risk to "Green" status?
1	Accidental alteration by agents of the School or those with whom we share data	Operational: Impact of errors, cost of investigation/correction People: incorrect decisions made, invalid payments/claims, excess work to correct Financial: errors may result in over/underspends, monies overpaid/underpaid; fines Reputation: loss of trust in School for reliability/accuracy Security: Invalid data in systems Regulatory: potential breach of GDPR if systems not in place to check.	5	3	15	Audit controls: Samples are regularly taken and reviewed for accuracy. Review controls: processes in place to review data for accuracy regularly. System controls: certain inputs not accepted, validation of key inputs.	3	3	9	No further controls are practicable; issues generally human error and this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
2	Deliberate alteration by agents of the School or those with whom we share data	Operational: Errors in service, cost of investigation/correction People: harm to individuals or profit from frauds Financial: alterations may result in financial fraud losses Reputation: loss of trust in School for reliability/accuracy Security: Invalid data in systems Regulatory: potential breach of GDPR if systems not in place to check.	3	3	9	Audit controls: Samples are regularly taken and reviewed for accuracy. Review controls: processes in place to review data for accuracy regularly. System controls: controls on access, controls on changes to DBMS systems Security controls: contracts, clarity on liability, policies and procedures	2	3	6	No further controls are practicable; this has been minimised as far as practicable
3	Accidental alteration by system error	Operational: Impact of errors, cost of investigation/correction People: incorrect decisions made, invalid payments/claims, excess work to correct Financial: errors may result in over/underspends, monies overpaid/underpaid; fines Reputation: loss of trust in School for reliability/accuracy Security: Invalid data in systems Regulatory: potential breach of GDPR if systems not in place to check.	2	4	8	Audit controls: Samples are regularly taken and reviewed for accuracy. Review controls: processes in place to review data for accuracy regularly. System controls: controls on system changes, formal testing processes.	1	4	4	No further controls are practicable; this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
4	Deliberate alteration by external agents	Operational: loss of access to data, cost of investigation/correction People: incorrect decisions made, invalid payments/claims, excess work to correct Financial: fraud; fines Reputation: loss of trust in School for reliability/accuracy Security: Invalid data in systems Regulatory: potential breach of GDPR/PCI if systems not in place to check	2	4	8	Role-based access control: only authorised persons are allowed access Location-based access control: access can only take place from some locations and trusted devices in many cases Security testing: penetration testing to discover potential vulnerabilities that malicious actors could exploit	1	4	4	No further controls are practicable; this has been minimised as far as practicable
5	Accidental destruction by agents of the School or those with whom we share data or incident affecting storage location	Operational: loss of access to data, potential loss of data, cost of investigation/correction People: delays in processing/payments, excess work to correct Financial: recovery costs, fines for late delivery Reputation: loss of trust in School for reliability Security: loss of data/resilience Regulatory: potential breach of GDPR if systems not in place to recover; potential breach of time-dependent compliance on other law	2	4	8	Business Continuity: Replication, resilient storage systems, backup systems Contractual: SLAs Security: RBAC to data	1	4	4	No further controls are practicable; this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
6	Deliberate destruction by agents of the School or those with whom we share data	Operational: loss of access to data, potential loss of data, cost of investigation/correction People: delays in processing/payments, excess work to correct Financial: recovery costs, fines for late delivery Reputation: loss of trust in School for reliability Security: loss of data/resilience Regulatory: potential breach of GDPR if systems not in place to recover; potential breach of time-dependent compliance on other law	2	4	8	Business Continuity: Replication, resilient storage systems, backup systems Contractual: SLAs, acceptable use policy Security: RBAC to data	1	4	4	No further controls are practicable; this has been minimised as far as practicable
7	Accidental destruction by computer system error	Operational: loss of access to data, potential loss of data, cost of investigation/correction People: delays in processing/payments, excess work to correct Financial: recovery costs, fines for late delivery Reputation: loss of trust in School for reliability Security: loss of data/resilience Regulatory: potential breach of GDPR if systems not in place to recover; potential breach of time-dependent compliance on other law	2	4	8	Business Continuity: Replication, resilient storage systems, backup systems Contractual: SLAs, acceptable use policy Security: RBAC to data	1	4	4	No further controls are practicable; this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
8	Deliberate destruction by external agents	Operational: loss of access to data, potential loss of data, cost of investigation/correction People: delays in processing/payments, excess work to correct Financial: recovery costs, fines for late delivery Reputation: loss of trust in School for reliability Security: loss of data/resilience Regulatory: potential breach of GDPR if systems not in place to recover; potential breach of time-dependent compliance on other law	2	4	8	Business Continuity: Replication, resilient storage systems, backup systems Security: RBAC to data, Virus/malware systems, firewalls	1	4	4	No further controls are practicable; this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
9	Accidental disclosure by agents of the School or those with whom we share data	Operational: loss of time in investigation/correction/publicity management People: damage to data subjects, potential risks of data abuse, excess work to correct Financial: fines for data exposure, damages for data exposure Reputation: loss of trust in School for security Security: disclosure of data Regulatory: potential breach of GDPR , investigation and action by regulator	5	4	20	Role-based access control: only authorised persons are allowed access Location-based access control: access can only take place from some locations and trusted devices in many cases Staff training and policy: training on data handling mandated for all staff and included in all data sharing agreements/contracts with those with whom we share data, with emphasis on controls of paper information which is most frequent issue Security reporting process: no-blame process to ensure where errors occur these are mitigated	3	4	12	No further controls are practicable; most issues with loss are paper and this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
10	Deliberate disclosure by agents of the School or those with whom we share data	Operational: loss of time in investigation/correction/legal action/publicity management People: damage to data subjects, potential risks of data abuse, excess work to correct Financial: fines for data exposure, damages for data exposure Reputation: loss of trust in School for security Security: disclosure of data Regulatory: potential breach of GDPR , investigation and action by regulator	2	4	8	Role-based access control: only authorised persons are allowed access Location-based access control: access can only take place from some locations and trusted devices in many cases Staff training and policy: training on data handling mandated for all staff and included in all data sharing agreements/contracts with those with whom we share data with disciplinary enforcement Contract controls: mandatory privacy in all contracts with potential penalties Security controls: malware controls, firewalls, protective monitoring	1	4	4	No further controls are practicable; this has been minimised as far as practicable

Risk Identification			Risk Assessment Gross or Inherent Risk			Existing Controls	Net or Residual Risk			Risk Treatment
Risk Ref	**Risk Title**	**Problem Description and Risk**	**Likelihood**	**Impact**	**Risk Score**	**Controls in place to mitigate risk**	**L**	**I**	**R**	
11	Accidental disclosure by system error	Operational: loss of time in investigation/correction/legal action/publicity management People: damage to data subjects, potential risks of data abuse, excess work to correct Financial: fines for data exposure, damages for data exposure Reputation: loss of trust in School for security Security: disclosure of data Regulatory: potential breach of GDPR , investigation and action by regulator	2	4	8	Role-based access control: only authorised persons are allowed access Location-based access control: access can only take place from some locations and trusted devices in many cases Security controls: malware controls, firewalls, protective monitoring, system testing	1	4	4	No further controls are practicable; this has been minimised as far as practicable
12	Deliberate disclosure by external agents	Operational: loss of time in investigation/correction/legal action/publicity management People: damage to data subjects, potential risks of data abuse, excess work to correct Financial: fines for data exposure, damages for data exposure Reputation: loss of trust in School for security Security: disclosure of data Regulatory: potential breach of GDPR , investigation and action by regulator	2	4	8	Role-based access control: only authorised persons are allowed access Location-based access control: access can only take place from some locations and trusted devices in many cases Security controls: malware controls, firewalls, protective monitoring, system testing	1	4	4	No further controls are practicable; this has been minimised as far as practicable