St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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	Likelihood 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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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 GDP, 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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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:	1	4	4	No further controls are practicable; this has been minimised as far as practicable

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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	
						mandatory privacy in all contracts with potential penalties Security controls: malware controls, firewalls, protective monitoring				

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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

St Andrew's C.E. Primary School

Article 35: Data Protection Impact Assessment – School Data Usage

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**	
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