	Name of School	**Corbets Tey School**
	Policy Review Date	**18th November 2020**
	Next Review Date	**Spring 2022**
	Reviewed by	**Governor Name: Julie Lamb** **Governor Signature:** 

Online Security Policy

Equality Impact Assessment

The school aims to design and implement services, policies and procedures that meet the diverse needs of our service, population and workforce, ensuring that no-one is placed at an unreasonable or unfair advantage over others.

Where the school is referred to in this policy, the policy and the following procedures apply to all staff working for Corbets Tey School on all sites including staff at the Routes4Life provision.

Strategic and operational practices

At this school:

- The Headteacher is the Senior Information Risk Owner (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. Key data and information asset owners are shown in Appendix 1.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff and governors are DBS checked and records are held in one central record in SIMS and on our Single Central Record.

  ALL of the following school stakeholders sign an Acceptable Use Policy (AUP) form that clearly outlines the responsibilities of the staff and visitors with regard to data security, passwords and network access.

  - Staff (including agency workers)
  - Governors
  - Parents
  - Visitors using the school network/Wifi

  Copies of AUPs are stored electronically in a secure folder on the school network.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require admin staff to change their passwords in SIMS (School Information Management System) and FMS (Financial Management System) termly. Admin nominated contacts are required to change their Unified Sign On (USO) password every 90 days.

- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution (RAV3) so teaching staff can access sensitive and other data stored on the school network from home, without need to transport data on mobile storage devices or laptops out of the school.
- School staff with systems administrator access, work within approved systems and follow the security processes required by those systems.
- We ask staff to undertaken annual digital housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical and manual solutions

- Staff have a personal secure area on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer and admin staff are automatically logged off if left unattended.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the secure AnyComms system to transfer CTF admissions data.
- We use Egress secure file transfer system to send and receive sensitive or confidential data files.
- We use pupils' initials wherever possible when transferring data or information in emails.
- We use Remote Desktop Protocol (RDP) for remote access to the school network and systems.
- We use London Grid for Learning (LGfL) Unified Sign On File Exchange (USO-FX2) to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, Atomwide's AutoUpdate, for creation of online user accounts for access to broadband services.
- LGFL offers a remote access platform with 2-factor authentication called Freedom2Roam.
- We use 2-factor authentication to access records in the Child Protection Online Management System (CPOMS).
- We store any Protect and Restricted written material in lockable storage cabinets in the school admin offices.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any internal back-up tapes in a secure server room. Back-ups are password protected. External back ups are encrypted and stored off site in JKloud high security data centres.
- We use JKloud remote secure back-up for disaster recovery on our Admin and Curriculum Networks.
- We comply with the Waste Electrical and Electronic Equipment (WEEE) Regulations 2013 on equipment disposal by using an approved or recommended disposal company for disposal of system hard drives, where any protected or restricted data has been held, and get a certificate of secure deletion for any hard drive that once contained personal data. This is arranged through Joskos Solutions who provide IT support and advice to the school.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder or disposed in confidential waste paper bins.

Appendix 1: Data and information assets

	Information Asset Owner	Who has access to enter information	Purpose
Pupil data (MIS)			
Core pupil data	Terence Hudson	Pupil Data Administrator	Teaching and learning /statutory returns
Attendance	Terence Hudson	Pupil Data Administrator	Teaching and learning /statutory returns
SEN	Terence Hudson	Pupil Data Administrator	Teaching and learning /statutory returns
EAL	Terence Hudson	Pupil Data Administrator	Teaching and learning /statutory returns
Exclusion, behaviour	Terence Hudson	Pupil Data Administrator	Teaching and learning /statutory returns
Reports and assessments	Terence Hudson	Head / Deputy / Class Teachers	Teaching and learning /statutory returns
Exam Data	Terence Hudson	Exams Officer / Deputy Headteacher	Teaching and learning /statutory returns
Tagged (named) student photos	Terence Hudson	Pupil Data Administrator	Teaching and learning /statutory returns
Child protection data	Emma Allen	Safeguarding Team	Teaching and learning /statutory returns
Staff data (MIS)			
Core staff data sets	Emma Allen	HR Administrator / Business Manager	Teaching and learning /statutory returns
Training and absence data	Emma Allen	HR Administrator / Business Manager	Teaching and learning /statutory returns
Finance system			
Purchase Orders, Invoices, Payments	Catherine Proctor	Finance Officer / Business Manager	Sound financial management
Approvals and budget setting	Catherine Proctor	Finance Officer / Business Manager / Headteacher	Sound financial management
Access control / passwords			
Authorise data access / Nominated Contacts	Emma Allen	Headteacher	Access to system(s)
Network password lists	Catherine Proctor	Business Manager / IT Technician	Access to system(s)
USO password information	Catherine Proctor	USO Nominated contacts	Access to system(s)
Email management	Catherine Proctor	USO Nominated contacts	Access to system(s)
Web filtering management	Catherine Proctor	USO Nominated contacts	Access to system(s)
Learning Platform password information	Sue Cumbers	USO Nominated Contacts	Access to system(s)

	Information Asset Owner	Who has access to enter information	Purpose
Disaster recovery			
Parental messaging system information	Catherine Proctor	Receptionist / Pupil Data Administrator / Business Manager	Business Continuity / communication
USO School Open Check	Catherine Proctor	Nomintaed Contacts / Business Manager / Headteacher	Business Continuity / communication
Managing back-up 'tapes' / automated system working	Catherine Proctor	Network manager / Joskoss Technician / Business Manager	Business Continuity / communication
Secure remote back-up	RedStor	Joskos Technician	Business Continuity / communication
Other potentially sensitive material			
Tagged (named) student photos	Catherine Proctor	Class teachers / Network Manager	Teaching and learning /statutory returns
Other personnel data (not in MIS)	Catherine Proctor	SLT / HR Officer / Business Manager	Business Continuity / communication
Learning Platform administration	Sue Cumbers	Class teachers / MLE SuperUsers	Teaching and learning /statutory returns
Assessment systems administration	Sue Cumbers	Class teachers / MLE SuperUsers	Teaching and learning /statutory returns
School website administration	Catherine Proctor	Administration staff / Business Manager / Head	Business Continuity / communication
Some Governors' documents	Catherine Proctor	Business Manager / Head	Business Continuity / communication
Performance management / capability papers	Catherine Proctor	Head / Deputy / HR Officer	Teaching and learning /statutory returns
Student medical reports / social service reports	Catherine Proctor	Head / Deputy / School Nurse / Class Teachers / Pupil Records	Teaching and learning /statutory returns
CCTV saved footage	*CCTV support company*	*automated system*	Safety / security
Information sent to parents	Emma Allen	Head / Deputy / Class Teachers	Business Continuity / communication