SEAHAM HIGH SCHOOL

Information Backup and Restore Policy

Contents

Review Date	Cycle	Reviewer	Adopted	Committee
December 2025	Annually	D Langlands	December 2025	Full Governors

Information Backup and Restore Policy

1 Introduction

Seaham High School has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. The school has a responsibility to ensure that information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances.

2 Purpose

The purpose of this policy is to identify and establish processes, procedures and good working practices for the backup and timely recovery of the school's information and data existing in both electronic and physical form.

3 Scope

The scope of this policy extends to the back-up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure.

4 Policy Statement

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice.

The following steps will help ensure the school's information and data is backed up and restored securely in the most efficient manner possible.

5 IT systems/data backups

1. The school's IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with the school's Disaster Recovery Procedures and departmental data retention policies
2. All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery
3. All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration

4. Where ever practicable backup media (e.g. tape) must be encrypted and appropriately labeled. Any system used to manage backed-up media should enable storage of date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster
5. A recording mechanism must be in place and maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc…) including any failures or other issues relating to the backup job
6. Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed
7. Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised
8. Access to the on-site backup location and storage safe must be restricted to authorised personnel only
9. All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media
10. Backup media must be protected in accordance with the school's Physical and Environmental and Data Protection and Media Handling Policies
11. Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the School's ICT systems. Where this may not be possible, photocopies of paper files must be made and stored in a secure storage location
12. Regular tests must be carried out to establish the effectiveness of the School's backup and restore procedures by restoring data/software from backup copies and analysing the results. Departmental IT Service Relationship managers should be provided with information relating to any issues with the backup testing of their data
13. Backup data/media no longer required must be clearly marked and recorded for secure disposal and with due environmental consideration (Waste, Electrical and Electronic Equipment - WEEE Directive).

User responsibilities

IT Users also have a responsibility to ensure School data is securely maintained and is available for backup:

1. Only encrypted USB data sticks should be used and any data stored must be for temporary purposes. All sensitive, business and personal identifiable information should be removed from the USB data stick and moved to an appropriate School data network location as soon as possible in order to ensure the data is made available to the school and can be successfully backed up
2. Mobile phones (not smart phones) must not be used to store sensitive, business or personal identifiable information. In the event of unforeseen or unavoidable situations leading to important data being stored on mobile phones, the data must be stored to a suitable school network location and removed from the phone as soon as possible.

Data restores

The School has well established backup and restore routines in place. Data (file) restores are normally carried out by the ITSS who will endeavour to restore files from a date specified by the user or from the nearest backed up date

1. IT Users must request data (files) to be restored by contacting the ITSS.
2. ITSS will need to verify that the User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/s. Content will be restored to the same source folder or the same area, so any requestor will need access to that folder/area to access the restored file.
3. Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:

    - The reason for the restore
    - The name of file/s and/or folder/s to be restored
    - Original location of file/s and/or folder/s - the Service Desk will provide guidance to the User on how to find this out
    - Date, day or time of deletion/corruption or nearest approximation
    - The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully

4. All backup and recovery (restore) procedures must be documented and made available to Data Centre personnel responsible for carrying out data (file) restores
5. Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen circumstance should be made under the supervision of ITSS.

6. Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required (applies to media from both school and remote storage locations)
7. A log must be maintained to record the use of backup media whenever it has been requested and/or used from secure storage.

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to school assets, or an event which is in breach of the school's security procedures and policies.

All school employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the school's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the School.

The school will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

This document forms part of the school's Data Protection Policy and as such, must be fully complied with.