BUXTON COMMUNITY SCHOOL

Information Security Policy 2019-20

Last Reviewed	Resource Committee 24.6.2019 F,P,P 11.15 24.06.2019
Reviewed by	Jayne McMillan Head of School Business & Resources
Next review date	July 2020

Information Security Policy

1. Background

Buxton Community School recognises that Information is fundamental to its effective operation and the purpose of this Information Security Policy is to ensure that the information managed by the school is appropriately secured in order to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

Failure to adequately secure information increases the risk of financial and reputational loss to the school. The school and its contents are at risk from potential criminal damage, theft and arson and potentially risks for staff and pupils and the data systems the school needs to function.

This policy should be read in conjunction with the schools Safeguarding, IT Policy and Data Protection Policy.

For the purposes of this document, 'the school' refers to Buxton Community School, SK17 9EA, as registered with the ICO.

2. Purpose

The objectives of this policy are to:

- Provide a safe and secure information systems environment for staff, students and any other authorised users.
- Ensure that all information and information systems within the School are protected to the appropriate level.
- Ensure that all users are aware of and comply with this policy and all current and relevant UK legislation.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Protect the school from liability or damage through the misuse of information or information systems.
- Ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

3. Scope

- The Information Security Policy applies to information in paper form, stored electronically or on other media, information transmitted by post, by electronic means and by oral communication, including telephone and voicemail.
- It includes text, pictures, audio and video.
- It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.
- Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

Information Security Policy

This policy applies to all staff, students and other members of the school and third parties who interact with information held by the school and the information systems used to store and process it, collectively termed 'users' throughout this document.

For the purposes of this document, information security is defined as the preservation of:

- Confidentiality (protecting information from unauthorised access and disclosure)
- Integrity (safeguarding the accuracy and completeness of information)
- Availability (ensuring that information and associated services are available to authorised users when required)

4. Availability and Access

Designated staff will be assigned responsibility for defining the appropriate use and ensuring that appropriate security measures are in place to protect data. (Designated staff are listed in Appendix 1)

All information will be classified according to a level of risk and retained / protected accordingly.

Information will be made available solely to those who have a legitimate need for access.

It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.

The integrity of information will be maintained.

Errors /omissions will be notified to the nominated owner and necessary amendments will be made in a timely manner, within the same working day where possible.

Information will be protected against unauthorised access and users will not allow non-nominated persons access or viewing rights.

Good security involves all school staff, teaching and non-teaching. All staff should know how to:

- Protect pupils from harm
- Safeguard Property
- Contact emergency services and implement emergency procedures
- Challenge anyone walking around the school without a lanyard or identification and escort them to reception if necessary.
- Ensure information systems they access are protected from unauthorised access and staff.
- Ensure they understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure information is disposed of in an appropriately secure manner when it is no longer relevant or used.
- Staff should report any concerns to the relevant designated staff or the DPO.

Information Security Policy

5. Designated Staff

Safeguarding Concerns / Pastoral Information	Jan Heron
SEND Records	Alex Garner
Unauthorised Access / Use IT Systems	Chris Carroll
Data Protection Breaches / Confidentiality Concerns	Heather Toomey
Unauthorised Access to Finance / Personnel Records	Jayne McMillan
Damage / Security Concerns in relation to the School Site / CCTV	Bevon Blackwood

6. Information Classification

Data is classified on the risks associated with its loss or misuse:

High Loss, misuse or unauthorised access to this data could result in significant financial loss, reputational loss and litigation.

Student data
Parental data
Staff data
Financial data
Staff to staff communications
Staff to third party communication such as the police / social services etc

Medium Loss, misuse or unauthorised access could result in reputational loss and litigation.
Teaching data
Background statistical data
Governance records
Communications relating to teaching groups / sets and ability

Low Loss, misuse or unauthorised access could result in reputational loss.

Management information
Public facing content
Day to day staff communications

7. Legal and Regulatory Obligations

The use of information is governed by a number of different Acts of Parliament. All users have an obligation to comply with current relevant legislation which includes, but is not limited to:

Computer Misuse Act (1990)
The Data Protection Act (1998)
Freedom of Information Act (2000)
Copyright, Designs and Patents Act (1988)
Regulation of Investigatory Powers Act (2000)
Human Rights Act (2000)
Electronic Communications Act (2000)
Digital Economy Act (2010)
Obscene Publications Act (1959 & 1964)

Counter-Terrorism and Security Act (2015)

8. Breaches of Security

Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the IT Manager immediately. They will advise on what steps should be taken to avoid or mitigate their impact, and identify action plans to reduce the likelihood of recurrence.

In the event of a suspected or actual breach of information security, the IT Manager, with or without consultation with the relevant department, may require that any systems suspected of being compromised are made inaccessible.

Where a breach of security involving either computer or paper records relates to personal information, the Schools Data Protection Officer must be informed, as there may be an infringement of the Data Protection Act 1998.

All physical security breaches should be reported to the Site Manager.

Where a crime is suspected / has been committed the Police may need to be called.

9. Policy Implementation and Disciplinary Procedure

All users are required to familiarise themselves with this policy and comply with its requirements.

An investigation of a suspected breach will endeavour to remain open minded and information will be sought from all relevant parties.

If a member of staff is found to have breached this policy, this may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken.

Failure of students to comply may lead to revocation of access and, in certain circumstances, legal action. The school may refer the user to the police where it reasonably believes a crime has been committed and will co-operate fully with any police investigations.

10. Associated Policies and Documents

The following policies support and provide additional context to this policy:

- Data Protection Policy
- Privacy Notice
- Freedom of Information Act
- Safeguarding and Child Protection Policy
- Acceptable Use Policy (Staff and Student)
- IT Policy
- Data Breach Notification Procedures

Information Security Policy

Information Security Responsibilities **ANNEX 1**

Strategic / Governor Data	Chair of Governors / Head Craig Yates
Finance	Head of School Business and Resources Jayne McMillan
Staff Data / HR	Head of School Business and Resources Jayne McMillan
Pupil Data	Data Manager / Admin Manager Heather Toomey / Sandi Flint
SEND Data	SENCo Alex Garner
Safeguarding	Designated Safeguarding Lead Lynne Pope
Pastoral Data Amy Meaden/ Claire O'Brien	DOP's / PM's Charlie Holman / Jess Lomas /
Medical Information	First Aider / School Nurse Anne Mulhall
I.T / Digital Data	I.T. Manager Chris Carroll
Exams Data	Exams Officer Janette Naden