Birkwood Primary School

Inspire

Cherish

Achieve

Together

INFORMATION SECURITY POLICY

UPDATED FEBRUARY 2022

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Birkwood Primary School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the school to achieve this, including to:

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

Introduction
Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Scope
The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of Birkwood Primary School, in whatever media. This includes: information held on computer systems, paper records, hand-held devices and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, governors and any and all third parties authorised to use the IT systems. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General principles
All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. All data so classified must be handled appropriately in accordance with its classification.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by Code Green or by such third party/parties as authorised.
The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with Code Green, unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to Mrs Suzy Gough, Bursar who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Physical security and procedures
Paper records and documents containing personal information, sensitive personal information, and

confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when desks are unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.
Available locked filing cabinets and locked cupboards shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform Mrs Suzy Gough as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Computers and IT
Responsibilities of the IT Consultant and Leadership Team
Code Green, in conjunction with the Leadership Team, shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;

b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's Senior Leadership Team, and reporting the outcome of such reviews to the School's Senior Leadership Team;

c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

Furthermore, Code Green, in conjunction with the Senior Leadership Team shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy;

b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;

c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;

d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];

e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;

f) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and

g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of staff
All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform Mrs Suzy Gough of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to a member of the Senior Leadership Team immediately.

Access security
All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teaches individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system. Passwords must be kept confidential.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see. Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Data security
Personal data sent over the school network will be encrypted or otherwise secured.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the School's requirements and instructions governing this use. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy).

Electronic storage of data
All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by Code Green.

Home working
All staff who are working from home should have security measures in place for their device e.g. laptop, tablet. This should include solutions such as encryption, virtual access or using cloud solutions. It is important that staff also follow these procedures:

- Ensure that they always log out, if leaving device unattended

- Put the device in a secure place in the home if they are not using it, where it can't be accessed by family members or visitors
- Always put the device in the car boot when moving between home and school
- Ensure that software updates are installed onto the device
- Log out of specific software when not using it

It is also recommended that they use their school-based device for any home working

Cloud Solutions – Sensitive Data
If using cloud-based solutions such as Google Drive, One Drive etc. to share resources and other documents with staff/parents/pupils, staff should ensure that additional security measures are put in place, particularly when storing very sensitive information:

One Drive Personal Vault – 2 factor verification:
https://www.microsoft.com/en-gb/microsoft-365/onedrive/personal-vault

Google Drive – Two Step Verification: https://www.google.com/landing/2step/

Live Streaming Lessons
If live streaming to a group of pupils, staff should ensure:

- The stream is monitored by another member of staff
- The member of staff is suitably dressed
- It is filmed in a suitable area of the house (not bedroom)
- It does not involve any other family members
- The background does not show any personal data e.g. photographs.
- The location services for the device are not enabled.
- A school-based device is used for the stream.

If staff are filming themselves, the above protocols should still be followed.

Live Streaming Meetings
The same protocols should be obeyed as have been stressed in the previous point. If schools are holding a governors meeting via live streaming, headteachers must ensure that all governors are following the conditions stated above.

Communications, transfer, internet and email use
When using the School's IT Systems you are subject to and must comply with the School's Acceptable User Policy.

The School work to ensure the systems protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to a member of the Senior Leadership Team.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery.

You should be careful about maintaining confidentiality when speaking in public places. You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Reporting security breaches
All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Mrs Suzy Gough / Mr Tim Pinto, Data Protection Officer. All members of staff have an obligation to report actual or potential data protection compliance failures. When receiving a question or notification of a breach, the Bursar shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Bursar or IT Lead Niall Sandwith.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to Mrs Suzy Gough.

All IT security breaches shall be fully documented.

Related Policies
Staff should refer to the following policies that are related to this information security policy:

- Acceptable User Policy
- Data Protection Policy

Monitoring and Review
The Governing Body reviews this policy every 2 years. The Governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the governing body receives recommendations on how the policy might be improved. This policy will be reviewed in February 2024.

Signed _____Headteacher Date _____

Signed _____Chair of Governors Date _____