ICKFORD SCHOOL

CYBER SECURITY POLICY

October 2022

Introduction

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.

Ickford 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 Pupil Privacy and 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;
- increase awareness and understanding at the School of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Confidential Data held in school

- Information concerning staff, students, parents, governors and partners.
- Unpublished financial information and contractual data

All employees are obliged to protect this data.

Protection of personal and school devices.

When employees use their digital devices to access school emails or accounts, there is an increased risk of the introduction of a security risk to our data. We advise all employees to keep both their personal and school devices secure.

The following should be applied:

- Keep all devices password protected.
- Ensure antivirus software is kept up to date.
- Ensure devices are not left exposed or unattended.
- Ensure that necessary security updates of browsers and systems are installed monthly or as soon as updates are available.
- Log into school accounts and systems through secure and private networks only.

All staff should avoid accessing internal systems and accounts from other people’s devices or lending their own devices to others.

All staff must read this policy alongside the:

- Pupil Privacy and Data Protection Policy
- Personal Data Breach Procedure
- School Workforce Privacy Notice
- e-Safety Policy

e-mail

Emails often host phishing attacks, scams or malicious software (e.g., trojans and worms.) To avoid virus infection or data theft, all staff should:

● Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., “watch this video, it’s amazing.”)

● Be suspicious of clickbait titles (e.g., offering prizes, advice.)

● Check email and names of people they received a message from to ensure they are legitimate.

● Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If there is any doubt that an email received is safe, staff should contact Stuart at WIBIRD our IT Technician.

Managing Passwords

Passwords should be secure so not to be easily accessed and should remain secret. Staff are advised to:

● Choose passwords with at least eight characters (including capital and lower-case letters,

numbers and symbols) and avoid information that can be easily guessed (e.g., birthdays).

● Remember passwords instead of writing them down. If there is a need to write passwords, any paper or digital document must be kept confidential and destroyed on completion of tasks.

● Exchange credentials only when absolutely necessary and avoid doing this electronically. Only exchange details in person and with trusted and verified contacts.

● Change passwords regularly.

Transferring Data

Staff must:

● Avoid transferring sensitive data (e.g. any data listed in the Pupil Privacy and Data Protection Policy, personal information, employee records and financial transactions) to other devices or accounts unless absolutely necessary.

● Only share confidential data via the school network system and not over public Wi-Fi or private connection.

● Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

● Report any data breaches, scams, privacy breaches and hacking attempt immediately to a senior staff member, the Trustee responsible for Data Protection or WIBIRD.

Additional measures

To reduce the likelihood of security breaches, staff should:

● Turn off their screens and lock their devices when not in use.

● Report stolen or damaged equipment as soon as possible to the Headteacher and WIBIRD.

● Change all account passwords at once when a device is stolen.

● Report a perceived threat or possible security weakness in school systems.

● Refrain from downloading suspicious, unauthorised or illegal software on school equipment.

● Avoid accessing suspicious websites.

We also expect our employees to comply with our E-safety Policy and associated policies.

Our Technical Support Company -WIBIRD

The school will work with WIBIRD to ensure that they can:

● Install firewalls, anti-malware software and access authentication systems.

● Support necessary security training to all employees as part of an initial induction and annually for existing staff.

● Inform the school regularly about new scam emails or viruses and ways to combat them.

● Investigate security breaches thoroughly.

● Help in maintaining this policy.

Working Remotely

Any member of staff working from home and accessing school information or data must have specific permission to do so.

Members of staff working remotely are obliged to follow all data encryption, protection

standards and settings, and ensure their private network is secure.

They must adhere to this policy and the E-safety policy when working remotely.

Action in the case of violations

All staff are expected to follow this policy and deliberate and serious breach of this policy may lead to disciplinary measures being taken in accordance with the School's disciplinary policy and procedure.

All of the School's phone, web-based, locally hosted systems and email related resources are provided for school purposes. Therefore, the school maintains the right to monitor all internet and local network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use or a risk to safeguarding.

Examples of deliberate or serious breaches of this policy and examples of misuse are, but not limited to:

- Knowingly disclosing login information to an unauthorised third party.

- Inappropriate disclosure of personal data.

- Knowingly installing software on Trust devices that hasn't been approved and which leads to a breach.

- Allowing the use of Trust devices by unauthorised third parties.

- Storing data on insecure media such as removable media that leads to a breach.

Safeguarding

Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and wellbeing.

Equalities Statement

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.