St. Andrew the Apostle Catholic Primary School

Acceptable Use Policy

December 2022

Succeeding Together in Faith and Love

Employee Responsibilities

Information security

I **must:**

- ✓ Take reasonable measures to protect all School information from unauthorised access, disclosure, modification, destruction or interference;
- ✓ Securely manage all information which is personal and/or confidential;
- ✓ Return all information and equipment in my possession at the end of my employment with the School;
- ✓ Immediately report any information security incident or weakness to a member of the senior management team (Information Asset Owner). If a member of the senior management team is unavailable then I must report it to the Head teacher;
- ✓ Assume responsibility for all visitors, escort them at all times when they are on School premises, ensure that the visitors log is completed and that visitor passes are obtained and then returned when they leave the premises;
- ✓ Ensure that windows are closed and locked when rooms are unattended and at the end of the working day;
- ✓ Lock away personal and/or confidential information when it is not required, especially when the room is vacated;
- ✓ Only print documents containing personal and/or confidential information using secure print facilities;
- ✓ Dispose of information securely and safely when no longer required;
- ✓ Dispose of paper which contains personal and/or confidential information by either cross cut shredding or place in a confidential waste bin;
- ✓ Dispose of all computers (including PCs, laptops and servers) memory sticks, CDs, and other electronic devices through the office;
- ✓ Take reasonable measures to protect paper documents that are taken outside of the school against unauthorised access, misuse or corruption;
- ✓ Take care when using electronic messaging, such as email, to transmit any form of information;
- ✓ Have appropriate authorisation to take away school assets including information, equipment and software from the school premises;
- ✓ Give information stored or processed outside of the school controlled location the same level of protection as it would have if worked on internally;
- ✓ Take all necessary precautions to prevent loss, damage or theft of information in my care;
- ✓ Ensure that encryption facilities are available and working on any IT equipment used for remote working;
- ✓ Ensure sensitive personal and/or confidential information is **only** ever sent by fax where there is no reasonable alternative AND risk to a child and/or the school if the information is not sent by fax. If sending a fax follow these requirements:
  - ✓ Confirm that you have the correct fax number for the recipient.
  - ✓ Care must be taken when dialling to ensure that the correct number is entered.
  - ✓ Before sending personal, sensitive and/or confidential information first confirm the presence of the specific recipient by ‘ringing ahead’ and asking the recipient to be ready to receive the fax.
  - ✓ Cover sheets must be used with all fax transmissions. The cover sheets must not be used to transmit personal, sensitive and/or confidential information, separate sheets must be used.
  - ✓ When a fax number is entered manually, the sender must visually check the recipient’s fax number against the cover sheet before starting transmission.
  - ✓ Once transmission is complete check the fax confirmation sheet to confirm that the receiving fax number and number of sheets are correct. Then telephone the intended recipient to confirm that they have received the fax in full.
  - ✓ If the confirmation sheets shows that it is not the correct fax number contact the recipient immediately by telephone if the number is available, or fax if not and ask them to destroy the original fax.

Information security

- ✓ Once you have sent and/or received a fax remove it from the fax machine immediately and do not leave it on the top of the machine to invite potential unauthorised access.

✓ Ensure that I follow these requirements if I am home working:

- ✓ Only take the minimum information home in order to do my work;
- ✓ Ensure that, where possible, I lock away personal or confidential information (for example information which if lost or stolen would cause an individual harm or distress);
- ✓ Ensure that I keep paper documents containing personal or confidential information separate from valuable items, for example remove from laptop bags, handbags, and so on;
- ✓ Ensure that when I leave my home, if school information is stored inside, I will lock all doors and windows and set a burglar alarm if one is fitted;
- ✓ Only take the information I really need with me. The more sensitive the document, the more care needs to be taken – if in doubt seek advice from your line manager
- ✓ Only take copies of paper files or electronic documents containing personal or confidential information home rather than originals, unless there is no alternative. Dispose of the information in a secure way when no longer required.
- ✓ Must not include identifying personal information on documents used to collect personal information unless absolutely necessary, for example when collecting information on vulnerable people;
- ✓ Must not leave paper or electronic files where they could be viewed by others, including family members;
- ✓ Must not put confidential or personal information in a domestic waste or recycling bin at home;
- ✓ Must not remove a paper file from the school unless absolutely necessary, permission has been given and it can be stored securely at home; and
- ✓ Must not use a personal (non-school) e-mail account for school business.

✓ Change my password if I think that someone else has seen it;

✓ Use the screen saver lock when working away from the computer (for Windows computers press CTRL+ALT+DEL and click on lock computer) or log out of my session;

✓ Secure a school laptop when it is left unattended i.e. by using a 'Kensington' (steel cable) lock or by locking it away in a cupboard;

✓ Store equipment, including laptops, out of sight in a locked cupboard overnight and at weekends if I don't take my laptop with me;

✓ Be aware of the environment around me and report any risks and/or concerns I have, for instance doors not locking.

✓ Keep paper files securely at all times;

✓ Always keep items close to me if using public transport;

✓ Place laptops out of sight in the boot and lock the boot if travelling by car;

✓ Not leave equipment and/or documents unattended (especially in vehicles). However, there may be exceptional circumstances where leaving a laptop in the boot of a car could be considered safer than carrying the equipment with you. In these instances you should carefully consider the risks involved as you will be asked to justify your decision, should there be a breach in information security.

I **must not**

- ☒ Ignore or exploit any information weaknesses;
- ☒ Let anyone avoid or bypass security by following me or another person through an access control door, unless you feel it is unsafe to do so. If you do feel unsafe and a person manages to gain access, inform the site manager and the Head teacher immediately; and
- ☒ Knowingly leave personal information on printing facilities including copiers, printers and faxes.
- ☒ Write my passwords down;
- ☒ Disclose and/or share my passwords with anyone;
- ☒ Use a word or phrase in a password that can easily be guessed – names, sports teams, and so on;

IT Acceptable Use

I **must**

- ✓ Save all data (including word documents and spreadsheets) to the appropriate fileserver;
- ✓ Only use encrypted portable storage devices (including laptops);
- ✓ Ensure that any electronic data authorised to be shared with a third party is undertaken in a secure manner approved by the school;
- ✓ Arrange all movements and redeployment of IT equipment through the school office;
- ✓ Notify my line manager, the Head teacher and the school office if any IT equipment is lost or stolen;
- ✓ Return IT equipment to my line manager or the school office immediately upon request;
- ✓ Report any suspicious messages and/or files to the IT Service Desk ,(*amend as appropriate*)
- ✓ Report any virus warnings to the IT Service Desk, *amend as appropriate*
- ✓ Use officially provided email addresses to send all business related emails. Officially provided email addresses include "@knowsley.gov.uk" and school provided office 365 email accounts;
- ✓ Follow the secure transfer protocol and where possible use encrypted email solutions (e.g. Egress Switch) when sending emails that contain sensitive personal and/or confidential information outside of the School's secure email service;
- ✓ Comply with the Data Protection Legislation for any data being transferred, especially when transfer is outside of the UK;
- ✓ Ensure that all recipients of an email are entitled/authorised to view the contents;
- ✓ Seek advice from my line manager, senior manager or Headteacher if I have any queries about business use of email
- ✓ Undertake personal use of email in my own time, ensure that such use is lawful and complies with the school's other policies and ensure that personal use of does not have a negative impact on the School or its partners; and
- ✓ Add the following disclaimer to all personal emails sent from School email facilities:

  "This email is personal. It is not authorised by, or sent on behalf of the school. This email is the personal responsibility of the sender."

I **must not:**

- ☒ Store personal and/or sensitive personal data on unencrypted portable / removable storage devices (including. laptops, USB drives etc.);
- ☒ Allow third parties to access any school information without confirming with my manager that they are authorised to have such access;
- ☒ Connect any non-school device to the Schools/Council's IT network without prior written authorisation from the Headteacher/Head of Information Technology (this includes devices owned by consultants, contractors and suppliers);
- ☒ Attempt to change any administration settings on computers that I use;
- ☒ Transmit by any electronic means any message, file or attachments which I know or suspect to be infected with a virus;
- ☒ Download any software (including screensavers) without the prior written approval of the Headteacher/Head of IT
- ☒ Forward virus warnings (unless requested to do so by IT dept.);
- ☒ Send or forward business emails or electronic files which contain personal and/or sensitive personal information to my home email address;
- ☒ Send emails to people if I am unsure if they are entitled/authorised to see the content;
- ☒ Use school email facilities for the transmission of unsolicited commercial or advertising material, chain mail or other junk-mail of any kind to colleagues or any other organisation;
- ☒ Create or transmit anonymous messages, i.e. without clear identification of the sender;
- ☒ Create or transmit material which could bring the school or its partners into disrepute;
- ☒ Send emails to large distribution groups without the authorisation of my manager;
- ☒ Send emails with large attachments without a legitimate business reason (5Mb is classed as large);

IT Acceptable Use

- ☒ Allow personal email use to interfere with performance or priorities of my or another person's duties;
- ☒ Conduct any form of private or third party business using the school's email service;
- ☒ Send excessive emails or large attachments; and
- ☒ Use business email addresses to register for personal websites (for example banks and online shopping), personal use of social networking sites or to confirm orders for personal goods or services.

Data Protection

I **must:**

- ✓ Follow the data protection principles which state that personal information must be:
  - ✓ processed fairly and lawfully;
  - ✓ processed for specified and lawful purposes;
  - ✓ adequate, relevant and not excessive;
  - ✓ accurate, and where necessary kept up to date;
  - ✓ not kept longer than is necessary;
  - ✓ processed in line with the rights of the information subject;
  - ✓ kept safe and secure; and
  - ✓ not transferred outside of UK unless in compliance with UK Data Protection Legislation.
- ✓ Adhere to any information sharing agreements that are in place for the school.
- ✓ Only provide the minimum amount of personal information necessary to respond to any lawful request; and
- ✓ Follow school procedures for requests for personal information (Subject Access requests)
- ✓ Comply with policies, procedures and guidance on the use of personal data.

I **must not**:

- ☒ Allow unauthorised access to any personal information; and
- ☒ Give personal information to anyone internally or externally, unless I am fully satisfied that the enquirer or recipient is fully authorised and legally entitled to the information.

As an employee of the School, you **MUST** read and understand your responsibilities as outlined in the key employee responsibilities document.

If you require further guidance on your responsibilities you must contact your line manager or the data protection officer.

Please sign below to confirm you have read and understood your responsibilities

Signature:

Role:

Date: