***Reynalds Cross Vision:***
*To be the best of the best; to be a place where "Every Individual" really does matter, to maximise independent learning and enjoyment in line with school aims; and to be a, positive, happy and fun learning environment with outstanding features.*

# Electronic Communication Policy

**Date adopted: 16th November 2021**

**Next Review date: November 2024**

Signed: _____
Chair of Governors

Signed _____
Head Teacher

**Introduction**

This policy contains important rules (in three sections) concerning the acceptable use by staff and security of the school's internet and email facilities, via the Solihull Grid which is provided by SMBC who are effectively the school's ISP (Internet Service Provider).

It is important to establish the rights and responsibilities of the individual member of staff to understand and accept this policy.

You must read this policy carefully and make sure you understand it. You will be asked to sign a form entitled **Staff Information Systems Code of Conduct** to say that you have read and understood it.

Information passing through or stored on school equipment can and will be monitored and used in line with Data Protection Act 1998 and Information Commissioner's Office and Human Rights Act 1998. Staff should also understand that Reynalds Cross School & SMBC reserve the right to monitor and review internet use and e-mail communication sent or received by employees as necessary to safeguard the School's interests and systems.

# STAFF INTERNET ACCESS

This section specifically covers access to the Web; the use of the internet for external e-mail is covered under the section **Email Use** and the general use of ICT equipment is covered under the section Staff **ICT Security**.

**Offensive Material**

You must not knowingly access, download or circulate pornographic, offensive, defamatory or other illegal material. This will be treated as a serious disciplinary offence, and may lead to dismissal. This includes loading files in an internet browser.

**Private use of the Internet**

Internet access is provided primarily for educational use. However, you are allowed to make private use of the internet in your own time providing that the school does not incur additional charges.

All parts of this policy still apply, including the prohibitions on accessing offensive material.

**Monitoring of Internet Access**

SMBC uses "filtering" software to block access to inappropriate sites. All internet access (successful or not, including personal use) is logged and can be tracked back to an individual workstation. Reynalds Cross School reserves the right to ask SMBC to inspect these logs and report to the school their findings. This will not happen unless there is a reasonable cause to believe that this or any other Reynalds Cross School or SMBC policies have been breached.

SMBC reserves the right to independently inspect the logs. Again, this will only take place where there is reasonable suspicion that SMBC policies have been breached or illegal activity taking place.

SMBC may use the log files to monitor and analyse overall traffic levels, and usage, including the most frequently used sites.

**Virus Checking**

The Internet Firewall will automatically check for viruses if information is downloaded from the Internet. Further protection takes place at school level, running local anti-virus software. However, there cannot be any guarantee that materials are virus free.

**Copyright**

Normal copyright laws apply; you must not download, use or distribute anything that is copyrighted unless you have a licence to do so (this applies to software, photographs and documents) – *see section ICT Security.*

**Downloading Files**

Where possible you should check the size of file before downloading. Be cautious about downloading any files above 2 megabytes. Large downloads will affect others on the school network.

**Financial Transactions**

You must not order goods or services for school over the Internet without proper regard to the Reynalds Cross School and SMBC Purchasing Policy and rules for contracts.

**Mailing Lists**

In order to limit the amount of junk mail coming into the Solihull Grid, only join mailing lists for legitimate reasons.

**Password Security**

Members of staff generally have individual login to access the Internet and E-mail. You must not use another person's individual login even if provided with it.

**Failure to comply**

You must observe the rules set under this section at all times; non-compliance may lead to disciplinary action and serious breaches of this policy may lead to dismissal.

**Use of Social Media**

There are various forms of social media, the list below is not endless but highlights examples of what we mean by Social Media for the purpose of this policy:

- social networking sites such as Facebook, Google+, Snapchat, Twitter and MySpace
- professional networking sites such as LinkedIn
- online chat rooms, forums and comments on web-articles or chat boards
- blogs, webcasts and wiki's
- online databases such as Glassdoor
- other social media such as YouTube and Flickr

'Use' of Social Media includes IT devices and locations not belonging to Reynalds Cross or SMBC.

- Staff must not engage in any activity or disclose information that brings or is likely to bring Reynalds Cross or SMBC into disrepute.
- When offering opinion or expertise on topics or employees of Reynalds Cross, ensure that care is taken to identify yourself, not disclose sensitive or confidential information; or post anything inflammatory illegal or under copyright.

Only authorised staff allocated to do so by the Head Teacher or the Chairperson of the FORCS committee are permitted to post material on a social media website in our name and on our behalf. Any breach of this restriction will amount to gross misconduct.

All communications we make using social media which promotes the school must have been through a formal approval process. Otherwise, you must not make any communication using social media which promotes our services. Any breach of these restrictions will amount to gross misconduct.

If you are in any doubt as to what you can and cannot say using social media, then please contact the Head Teacher or SMBC HR Department.

**Rules for use of Social Media**

We are not suggesting that you should stop using social media, but to think more about the consequences of anything that you post onto a Social Media website.

You should comply with the following basic rules whenever you are using social media sites, whether using our equipment or your own equipment and whether you are doing so during or outside of working time or whether you are on school premises or in a school related environment:

- Always write in the first person, identify who you are and what your role is, and use the following disclaimer "The views expressed are my own and don't reflect the views of my employer".
- When using social media sites such as Facebook, MySpace, Google+, Twitter, YouTube, blogs etc you are operating in a public space and your conduct may have serious consequences for the school, its employees, its pupils, and other affiliates.
- Conversations between 'friends' on Facebook and Twitter are not truly private and can still have the potential to cause damage. Remember also, that your comments can be copied or forwarded on to others, without your permission. Do not rely on privacy settings.
- Don't discuss colleagues, pupils or any other affiliates of school, without their prior approval.
- Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.
- Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any employee who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Head Teacher or SMBC HR Department.

- Never disclose sensitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with your Line Manager. In particular if you have colleagues or affiliates on your profile, make use of grouping 'friends' and amending your privacy settings by group of people.
- Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.
- It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticising it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.
- Before you include a link to a third party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.
- When making use of any social media platform, you must read and comply with its terms of use.
- Do not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.
- Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of us as a school. If you make a mistake in a contribution, be prompt in admitting and correcting it.
- You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.
- Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.
- If you feel even slightly uneasy about something you are about to publish, then you shouldn't do it. If in doubt, always discuss it with your Line Manager first.
- Do not post pictures of yourself wearing uniform or presenting your ID badge unless this projects a positive image of the school.
- Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.
- Before your first contribution on any social media site, observe the activity on the site for a while before launching in yourself to get a feel for the style of contributions, the nature of the content and any 'unwritten' rules that other contributors might follow.
- Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.

If you notice any content posted on social media about us (whether complementary or critical) please report it to the Head Teacher or SMBC HR Department.

**Use of LinkedIn**

If you have a LinkedIn profile then you must ensure that, whenever your profile relates to your employment at Reynalds Cross School and the following guidelines are adhered to:

- It is accurate
- It does not divulge confidential or sensitive material, or material which might lower the reputation of the school
- You refer to the school and your employment in a way which is respectful

- If you make a personal recommendation for someone, you could find yourself liable for so-called 'personal' references (in other words, an employee vouching for a colleague in a personal capacity). This includes giving personal recommendations or testimonials on LinkedIn or other social media.

**Recruitment**

We may use social networking sites as recruitment aids and during candidate attraction, but we will adhere to the following guidelines:

- Searches will not be carried out before candidates have been shortlisted for interview
- We will warn candidates that we conduct searches of social media sites as part of our decision-making process
- Searches will be limited to what ostensibly looks like material that is relevant to the candidate's ability to do the job
- Candidates will be permitted to comment on any information which causes us to reject a candidate's application.
- Information about a candidate's gender, ethnic origin, age, sexual orientation, disability, religion or pregnancy which is revealed through any searches will not be used or disclosed.
- Under no circumstances will the information gained be used to discriminate against job applicants in contravention of our equality policy.

# E-MAIL USE

Use e-mail wisely, especially with matters of a sensitive nature. There are many situations where a telephone call or face-to-face conversation is more suitable.

**E-mail Monitoring**

All e-mail (including personal e-mail) is logged and the School reserves the right to ask SMBC to present to them the contents of any e-mails you send or receive. This request must come from either the Head Teacher or an official representative of the Governing Body. SMBC do not routinely look at e-mail content, however they may, in the course of their work, be able to see addresses.

All e-mails are filtered for inappropriate or abusive words.

Reynalds Cross School will not request this inspection unless there is a reasonable suspicion that this, any other school or relevant SMBC policy has been breached.

However, there may be occasions when it may be necessary to give others access to your mailbox e.g. when absent from work.

SMBC may independently choose to inspect e-mail where they have reasonable suspicion that SMBC policies are being breached or that an illegal activity is taking place.

SMBC may also log files to analyse overall traffic and usage. They have backup routines that mean that deleted e-mails can also be retrieved.

**Disclaimer**

The following disclaimer is automatically added to all email sent to external organisations, not to other establishments within the Solihull Grid:

"*This email and files transmitted with it are confidential and intended solely for the use of the individual to whom it is addressed. If you are not the intended recipient please notify the sender immediately and delete the message. Any views or opinions expressed are solely those of the author and do not necessarily represent those of the school, establishment or Solihull Metropolitan Borough Council unless explicitly stated otherwise"*

*"The School, establishment or Solihull Metropolitan Borough Council may monitor the content of email sent and received via its network for the purpose of ensuring compliance with its policies and procedures."*

**Failure to Comply** – *see section ICT Security for further information*

Failure to comply with the rules set out under this section may:

- Result in legal claims against you, the School and SMBC.

- Lead to disciplinary action being taken against you, including dismissal for serious breaches of the policy.

**Rules** – *See section ICT Security for further information*

What you must:

- All staff will be given a unique **username and password** (be aware that if you give someone else this information they could send an e-mail that would be tracked back to you).
- The Data Protection legislation applies to email: only relevant and accurate information about individuals should be included in emails and attachments.
- The central Solihull Grid system will automatically check for viruses in the messages and attachments or incoming and outgoing external email. You may receive a virus warning email – most are hoaxes do not circulate but forward it to support@solgrid.org.uk, who will investigate and evaluate the risk.
- You should still exercise caution where viruses are concerned. New viruses are released all of the time and although all reasonable steps are taken there is no guarantee that one will not get through.
- Remember that although email tends to be more informal than conventional written communication, once sent it is equally formal and undeniable. If you usually require permission to send conventional mail then you will need to ensure you have similar authorisation to send to external organisations.

**You must not:**

The school will not tolerate the unauthorised use or misuse of its systems. Violations of IT services use include, but are not limited to, the following:

- Any message that could constitute bullying or harassment.
- Staff must only use their own username and password, and should not disclose these for use by anyone else.

- You should periodically change your password.
- You must not send abusive messages or message attachments that contain sexual, sexist or racial material.
- You must not send or circulate, internally or externally, any information which is defamatory.
- Gambling or illegal activities.
- Accessing, downloading, uploading, saving, receiving or sending material which:
    - Has sexually explicit content
    - Contains images of nudity
    - Contains material using vulgar, sexist, racist, threatening, violent or defamatory language.
- Posting or disclosure of confidential information about other employees, the school or its affiliates
- Personal use (to excess) e.g. social invitations, personal messages, jokes, cartoons or send or receive chain letters.
- Installing software without prior approval.
- Connecting devices or storage media to school equipment without prior approval e.g. usb keys and disks, cds, dvds
- You must not circulate software or any other material that may be copyrighted
- Connecting non-school computers to the network is not appropriate.

**Good Practice and General Guidelines**

- Do not open emails or attachments from sources you do not trust. Many macro-viruses are delivered via email attachments. If there is any doubt contact your ICT co-ordinator or person with delegated responsibility.
- You should not send any highly confidential documents externally via email
- Ensure that individuals or organisations that may send you email know your correct email address. Incorrectly addressed incoming mail will be returned to the originator. SMBC cannot open emails to forward them as this could be seen as a breach of the Human Rights Act.
- Only join mailing lists for legitimate business/educational reasons it limits the junk mail coming into SMBC which would continue when you left. It also unnecessarily increases the load on the system.
- When forwarding messages consider whether the originator of the message would be happy for this to be forwarded. If you alter any forwarded text make it clear that you have done so.
- Be aware of “Netiquette” for example sending a message in capital letters as this could be interpreted as “Shouting” at the recipient. In addition, be mindful of using familiar terms and emoji’s in professional emails.
- Be mindful that Flame-mails’ (e-mails that are or could be deemed to be abusive) can be a source of stress and can damage work relationships. Hasty messages, sent without proper consideration, can cause unnecessary misunderstandings.
- The style and content of an e-mail message must be consistent with the standards that the school expects from written communications:
    - Always include a subject line to indicate content and purpose.
    - Use correct spelling, grammar and punctuation.
    - Use sentence case correctly.
    - Do not over use colours or graphics as many users’ email applications cannot display them.
- Do not write anything slanderous in your emails

# ICT SECURITY

Computer security is very important. With the increasing reliance on computer-based systems, the security and confidentiality of information becomes more important. As some computer crimes are now criminal offences, prison sentences can be imposed. As well as the person committing the crime, the Head Teacher or Chair of Governors could also be charged.

It is important to recognise the variance in sensitivity of information held on the school computer systems. Processes need to be put in place to prevent all information having unauthorised access. Someone unnecessarily viewing information on the screen is "unauthorised access". The processes need to take into account how sensitive the information is.

Information produced by pupils in the course of their work is covered by the Data Protection Act.

All data needs to be secured against loss or corruption, particularly confidentiality of staff and pupil information.

This document is relevant to all staff and all ICT systems irrespective of the equipment in use. Many of the requirements are common sense and people may assume they are already in use. Unfortunately only if something goes wrong will the weaknesses then become apparent.

This policy applies to all laptops, workstations, photographic equipment, networks and ICT systems; both curriculum and administrative that are maintained both on and off school premises.

**Objectives**

The main objectives of this section of the policy are:

- To ensure that all the school's assets, staff, data and equipment are adequately protected on a cost-effective basis against any action that could adversely affect the ICT services required to conduct their work.
- To ensure that staff are aware of and fully comply with all relevant legislation.
- To create and maintain within Reynalds Cross a level of awareness of the need for ICT security to be an integral part of day to day operations so that all staff understand the need for ICT security and their own responsibilities.

**Responsibility**

It is the responsibility of the Head Teacher and the Governing Body to ensure the provision of adequate security for all computer equipment and data locked in school.

All or part of this responsibility may be delegated to other members of school staff.
Reynalds Cross School has a designated member of staff with the responsibility for Data Protection and computer security. Throughout this policy, Reynalds Cross School refers to the person discharging their responsibilities where appropriate.

Reynalds Cross School has a duty to monitor computer activity to ensure that:

- Computer usage is legitimate.
- Only licensed software is used.
- All procedures comply with any relevant UK legislation, for example the Data Protection Act, Copyright Act and Computer Misuse Act.
- All staff are aware of their security responsibilities.
- Access is set at appropriate levels of security.
- Access rights are cancelled as soon as a member of staff leaves.

It is the duty of all school staff to report any misuse of software or abuse of computer equipment. This would be to: the Head Teacher, designated person or Data Protection Officer at SMBC.

Internal Audit and Data Protection Officers from SMBC will carry out checks to ensure that the overall policy concerning ICT security is followed.

**Computer Equipment**

All computer equipment must be adequately protected against theft, fire, malicious damage or unreasonable environmental surroundings. Access to restricted areas should be confined to authorised persons. Access devices such as keys, card keys, passwords or codes must not be transferred to another unauthorised person.

The physical security of each piece of computer equipment in Reynalds Cross School is the responsibility of the Head Teacher or designated staff member who should consider the use of appropriate physical security to include security marking, with at least the postcode, and where necessary physical devices i.e. lock or cage.

Workstations should be placed in positions that only allow the screen's display to be seen by authorised staff. A screensaver providing immediate complete screen confidentiality should be used in conjunction with a password – ideally it should be set to activate after a maximum duration of 10 minutes.

All confidential output must be stored securely when not in use. Waste computer printouts, floppy discs etc., must be disposed of in a secure manner i.e. shredded. It is the responsibility of the Head Teacher and Governing Body to provide adequate facilities for the disposal of computer waste.

Where computer equipment may be removed from buildings e.g. for use at home:

- Prior approval in writing must be obtained from the school, specifying the reason for removal and duration. Reynalds Cross School will ensure the timely return of the equipment and check that no damage has occurred.
- All of the provisions in this section of the policy equally apply and laptops will need particular consideration and care should be taken not to expose them to the likelihood of theft.

**System Security**

- Workstations must not be connected to networks or allowed access to specific systems until agreed by the person with delegated responsibility.

- Workstations must be logged off immediately after use. If a workstation has more than one “window” each screen must be logged off separately.

- If appropriate, password security must be used on all computers and applications (i.e. where personal/sensitive data is stored).

- Laptops will need particular consideration where sensitive information is stored a. Individual documents must be password protected b. Encryption software may be necessary.

- Whenever possible passwords must be used by only one person, changed regularly, and not disclosed to other persons. A password should be specific to a person at least six characters long and should not be written down. Group or shared passwords should only be used in exceptional cases and should give restricted access to the systems they control.

- Particular attention should be paid to pupils passwords, particularly if using email.

- The IT technician/co-ordinator must be informed when persons leave or change posts so as to amend or remove their access immediately. Anyone who thinks their password is known by another person should change it immediately.

- Copies of computer files must be taken regularly. The Back up system operated within Reynalds Cross School is done at the end of the day Monday – Friday during term time. The Head Teacher may delegate this responsibility to a staff member. Copies of the back up tapes are stored in the school safe and rotated with four x Friday tapes and one for each day.

- SMBC provides an internet access and email logging system for Reynalds Cross School in line with email and internet policies.

**Privacy**

Every effort must be made to ensure that confidential information can only be accessed by persons who have authorisation to view it.

Staff must be aware of the implications of the Data Protection Act.

At Reynalds Cross School, the Head Teacher or the designated member of staff has the responsibility for ensuring that we comply with the Data Protection Act. One duty is to review Reynalds Cross School’s register entry and to notify the Data Protection Officer at SMBC of any changes.

Appropriate training should be given for this role and responsibility.

**Software Piracy**

All software loaded on Reynalds Cross School computer systems must have been agreed with the Head Teacher and SMBC. It is a criminal offence to “Pirate” software.

Personal software should not be loaded onto Reynalds Cross School computers under any circumstances. If software is deemed to be of use then it should be duly acquired under licence.

Loading any borrowed software onto Reynalds Cross School computer systems is a disciplinary matter and a criminal offence.

**Software Viruses**

Viruses, programs that can corrupt computer files are a real threat to computer systems. To minimise the risk of infection SMBC provides virus software run on Reynalds Cross School computers.

All PC's (including laptops) should be protected by virus protection software. Any detected viruses must be reported to SMBC immediately.

All disks/CD ROMs should be virus checked prior to use in any Reynalds Cross School computers. Especially where they have been received from an external source.

Disks/CD ROMs must not be inserted into PCs until after the boot password has been entered and the computer has either reached:

- The point where you log onto the network or
- The Windows screen on stand alone computers; unless
- The disk is supplied by SMBC and the designated person is instructed to use it as a boot disk.
- Failure to adhere to the above will mean that the Disk/CD ROM is not scanned for viruses.

**CCTV**

The school maintain and operate closed circuit television (CCTV) cameras within designated facilities throughout the school. This policy will enable all persons who use, or come into contact with, CCTV recording equipment, be reassured that it is being used in the correct manner.

- Provide clear and unambiguous information on the use of CCTV recording equipment used by Reynalds Cross
- Provide a framework of instructions for the use, retention, and analysis of CCTV recordings.
- Meet the requirements of the Data Protection Act.
- Meet the requirements of the Health and Safety at Work Act.
- Promote a safer working environment for staff, pupils and visitors and any other persons who may come into contact with the CCTV recording system used by Reynalds Cross.

**Disaster Recovery**

Security copies are taken every night (Monday – Friday) and stored in the Office safe.

Acquisition and Disposal of ICT equipment.

All purchases and disposals should be made in accordance with Reynalds Cross School and SMBC financial regulations and policies.

All purchases of computer equipment should take account of security requirements.

The physical security of equipment must take account of the guidelines earlier in this policy under “Computer Equipment”.

All personal or sensitive data must be removed prior to disposal of any ICT equipment.

**Intellectual Rights**

Reynalds Cross School agrees to respect the intellectual ownership of software. If it is licensed, the licence agreement will be respected and unauthorised copies will not be made.

Reynalds Cross School and SMBC claims the rights to all software developed for the school or SMBC by its employees and by persons acting as its agents.

All computer programs developed for Reynalds Cross or SMBC are the property of SMBC. All data, except that held for other agencies, is the property of SMBC.

**Personnel Policy**

Any employee knowingly breaching this section of the policy may be subject to disciplinary proceedings.

These breaches include:

- Use of another member of staff’s password.
- Unauthorised disclosure of information.
- Deliberate and unauthorised access to, copying of, alteration to or interference with computer programs or data.
- Loading “Pirate” or borrowed software.

If a member of staff resigns or is either suspended or dismissed, the security of computer equipment and data should be considered.

All staff will be provided with enough information to comply with this Policy. A copy will be available to all employees. It will be explained at induction courses for new staff and refresher training will be available.

It is the duty of all members of staff to report any suspected irregularities/fraud to either the Head Teacher, Chair of Governors or Internal Audit at SMBC as soon as possible. Such information will be regarded as confidential by all employees involved.

If you have any queries about this policy please contact the Head Teacher, SMT or Chair of Governors, or the person with designated responsibility or the Council Data Protection Officer at SMBC.

Reynalds Cross School are obliged to adopt this SMBC policy as part of our legal duty to safeguard our pupils from harm and it will be amended as and when the SMBC state that change makes it necessary.

**Relevant Computer Security Legislation**
*(Copyright and Software Acts)*

The UK *Copyright Designs and Patents Act 1988* and the European Software *Directive (91/250/EEC)* say that you may not copy, adapt or distribute a computer program in any way without the permission of the publisher.

This includes:

- Making physical copies of the software.
- Making electronic copies on your computer or in a local network.
- Making copies from the internet or other interactive network.

The *Copyright Designs and Patents Act 1988* and the *Trade Marks Act 1994* are acts which allow authorities to:

- Prosecute offenders with a criminal charge.
- Allow the copyright holder to enforce their own rights in a civil court.

Possible penalties in Criminal Courts: Imprisonment for up to ten years, substantial fines, confiscation of assets. Possible penalties in Civil Courts: Injunctions to stop any further use of the software and to delete or hand over illegal copies, payment of damages, payment of court costs.

The *Computer Misuse Act 1990*
This act was introduced after the Law Societies of the UK recommended the need for legislation to cover the growing threat of computer crime. It identified three new offences; **Unauthorised access** – "Hacking" or eavesdropping where the contents of computer files are not modified. **Ulterior Intent** – Extends legal power to include both use of a computer to commit an offence and also where it aids the committing of another offence. **Unauthorised Modification** – an offence is committed if any action by the offender causes unauthorised modification of the contents of the computer with the intention of disrupting or damaging its' contents.

The *Data Protection Act 1984*
This was passed to ensure that the increasing use of computers and other electronic data storage is not subject to abuse. The Data Protection Act is concerned with the protection of personal data. The keys points of the Act are:

- To protect personal data and to require all personal data to be processed in accordance with a number of principles.
- To require organisations that process personal data to register that fact, and then only process data in accordance with the terms of registration.

Anyone can inspect the Register and request to see data held on them. If the data held is inaccurate the data subject can take steps to rectify or delete it. Personal data is defined as data that is held on a living individual who can be identified from the data itself. Some personal data is exempt from registration: Data held only for payroll purposes, accounting data, data that could compromise national security, data that is already public information, held by individuals concerned with personal, family or household affairs, held for recreational purposes, held by an incorporated members club relating to members of the club, held for distribution purposes, data processed outside the UK.

# STAFF INFORMATION SYSTEMS CODE OF CONDUCT

**To ensure that staff are fully aware of their professional responsibilities when using school information systems, they are asked to sign this code of conduct.**

**Staff should consult the Staff Internet Access, Email Use and ICT Security Policy in school for further information and clarification.**

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that the school and SMBC may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system administrator.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or assessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concerns regarding pupil safety under this policy to the Head Teacher or the designated Child Protection Officer, and I understand the use of CCTV
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote information system safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand the school and SMBC's policy on use of social media.

*The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place; or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. I understand that any breach could lead to disciplinary action.*

**I have read, understood and agree with the Information Systems Code of Conduct.**

Print Name: ……Signed: ……Date: ……...

Accepted for school: ……Print Name: …..……..