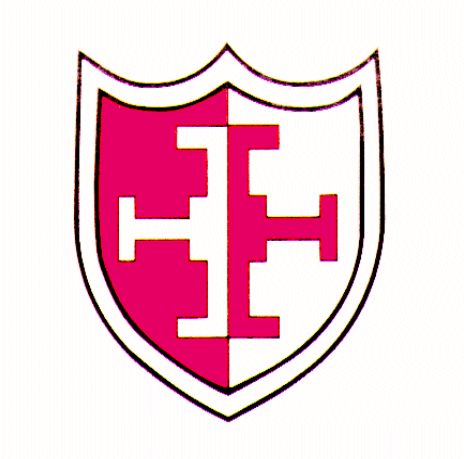
**ST. CHAD'S CATHOLIC PRIMARY SCHOOL**



***'Christ in our heads, our hearts, our hands'***

# E-SAFETY POLICY

**March 2019.**

**SCHOOL E-SAFETY POLICY**
**INTRODUCTION**

1. **This Policy applies to all employees of the School, the Governing Body, volunteers, visitors and members of the public on School grounds.**

2. The internet and e-mail play an essential role in the conduct of our business in school. The systems within school are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been a substantial investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.

2.1 How we communicate with people not only reflects on us as individuals but on the School. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of e-mail and the internet.

2.2 We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

2.3 For your safety, we are able to monitor all web pages visited, emails sent and emails received. This helps us monitor inappropriate use, such as bullying.

2.4 This policy applies to you as an employee whatever your position, whether you are a Head Teacher, Teacher, Support staff, permanent, temporary or otherwise. Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. (See also Staff Behaviour policy).

2.5 It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Principal or your line manager.

2.5.1 Every adult who has access to the computers in school must sign a "Staff Acceptable Use Policy" (Appendix 1).

2.5.2 Every child must sign the "Rules for Responsible Internet Use – or Primary Pupils" (Appendix 2)

2.5.3 During the logging process every user will have to accept the appropriate Acceptable Use Policy.

3. **GENERAL PRINCIPLES AND LEGAL ISSUES**

3.1 All information relating to our pupils, parents and staff is confidential. You must treat all School information with the utmost care whether held on paper or electronically.

3.2 Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.

3.3 We trust you to use the internet sensibly. Please be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school.

3.4 The main advantage of the internet and e-mail is that they provide routes to access and disseminate information; however, the same principles apply to information exchanged electronically, which applies to any other means of communication.
For example, sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

3.5 Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of the Principle.

3.6 As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School where it is necessary for your duties. The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

3.7 Staff must seek to reduce the risk of losing information and should exercise due care and vigilance when handling data. Therefore, employees must not keep information that relates to the learners identity on USB memory sticks.

3.8 All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

4. **MONITORING COMMUNICATIONS**

4.1 This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

4.1.1 to establish the existence of facts

4.1.2 to ascertain compliance with applicable regulatory or self-regulatory practices or procedures.

4.1.3 to ascertain or demonstrate effective system operation technically and by users.

4.1.4 for national security/crime prevention or detection.

4.1.5 for confidential counselling/support services.

4.1.6 for Investigating or detecting unauthorised use of the system

4.1.7 for monitoring communications for the purpose of determining whether they are communications relevant to the business.

4.2 Through Research Machines (RM) the school has a contract with E-Safe Forensic monitoring to monitor the use of the internet and e-mail services provided as part of DGfL, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in

disciplinary procedures if necessary. RM, and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications.

4.3 If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

4.4 Emails should be encrypted if they contain information about a named child or adult.

4.5 Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

4.5.1 providing evidence of business transactions;

4.5.2 making sure the School's business procedures are adhered to;

4.5.3 training and monitoring standards of service;

4.5.4 preventing or detecting unauthorised use of the communications systems or criminal activities;

4.5.5 maintaining the effective operation of communication systems.

## 5. **USE OF INTERNET AND INTRANET**

5.1 When entering an internet site, always read and comply with the terms and conditions governing its use.

5.2 Do not download any images, text or material which is copyright protected without the appropriate authorisation.

5.3 Do not download any images, text or material which is inappropriate or likely to cause offence.

5.4 If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.

5.5 If you are involved in creating, amending or deleting our web pages or content on our web sites, such actions should be consistent with your responsibilities and be in the best interests of the School.

5.6 You are expressly prohibited from:

5.6.1 Introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;

5.6.2 seeking to gain access to restricted areas of the network;

5.6.3 knowingly seeking to access data which you are not authorised to view;

5.6.4 introducing any form of computer viruses; and

5.6.5 carrying out other hacking activities.

5.7 For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

5.7.1 unauthorised access to computer material i.e. hacking;

5.7.2 unauthorised modification of computer material; and

5.7.3 unauthorised access with intent to commit/facilitate the commission of further offences.

## 6. **USE OF ELECTRONIC MAIL**

6.1 You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.

*6.2* Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line

6.3 Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.

6.4 Do not impersonate any other person when using e-mail or amend any messages received.

6.5 It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

6.6 Staff should ensure that they actively sign out of online services, portals or sites which contain sensitive information or access to emails.

## 7. SOCIAL NETWORKING

When using school approved social networking sites the following statements apply:

7.1 School equipment should not be used for any personal social networking use.

7.2 Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.

7.3 It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @st-chads.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school

7.4 Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

7.5 Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm

7.6 The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way

7.7 Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries.

7.8 Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them

7.9 Employees must ensure they do not breach the schools Information Security policy and staff behaviour policy when using social networking.

8. **DATA PROTECTION**

8.1 Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must:

8.1.1 Keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager; use of the One Drive or CC4 will enable secure access at home or school. **Flash drives are not to be used** for reports/images/sensitive information as they can be easily lost or stolen.

8.1.2 Familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;

8.1.3 Familiarise yourself with all appropriate School policies and procedures;

8.1.4 No personal or other inappropriate remarks should be made about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

8.2 The School views any breach of the Data Protection Act 1998 as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.

8.3 If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

8. 4 Refer to appropriate guidance found in GDPR/ Data protection policies.

**Appendix 1**

## St. Chad's Catholic Primary School.

## Staff Acceptable Use policy

## Rules for Responsible Internet use

This policy applies to all adult users of the schools systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

### Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.

- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not :
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

**Electronic Mail**

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.
Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.

- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

**Social networking**

When using school approved social networking sites the following statements apply:-

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @st.chads.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

**Data protection**

The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must:-

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed:……

PRINT NAME……

Dated: ……..

**Appendix 2.**

## St. Chad's Catholic Primary School.

## Rules for Responsible Internet Use

## For Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

**I agree that:**

I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network I will check with my teacher to see if it is possible.

***I am aware of the CEOP report button and know when to use it.***

***I know anything I do on the computer may be seen by someone else.***

**Signed:……**
**PRINT NAME……**
**Dated: ……..**