ST ALBAN'S CATHOLIC PRIMARY SCHOOL

Christ Be Our Light

Acceptable Use Policy (AUP) for School Staff & Governors

Autumn 2020

This Policy will be reviewed in Autumn 2021

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Networked Resources
These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources.

All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility
Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the E-safety officer

Acceptable Use
Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact the E-safety office
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Staff or students finding unsuitable websites through the school network should report the web address to the E-safety officer
10. Do not introduce USB memory sticks into the network without having them checked for viruses.
11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity, all sites visited leave evidence in the

county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
13. Files held on the school's network will be regularly checked by the E-safety officer
14. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting (See sections 8.0 in the WSCC ICT in schools Acceptable Use Protocol guidance).
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data. (See section 9.0 respectively in the WSCC ICT in schools Acceptable Use Protocol guidance).
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from the ICT subject leader

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the E-safety officer immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

Media Publications
Written permission from parents or carers will be obtained before photographs of pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- the school website
- the Local Authority web site
- web broadcasting
- Newspapers

Pupils' work from which the pupil can be identified will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.

EMAIL

- E-mail is not guaranteed to be private. Any suspected unauthorised use of the email system will be investigated to ensure compliance with these Protocols. Messages relating to or in support of illegal activities will be reported to the authorities.
- Anonymous messages should not be sent.
- Messages that are likely to bring the school into disrepute should not be sent.
- Excessive social e-mail use can interfere with learning and may be restricted. (Incidental personal use is permitted provided it complies with these protocols and does not interfere with work or study).
- Access in school to external personal e-mail accounts may be blocked.
- The forwarding of chain letters is not permitted.
- Official E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Do not open suspect emails or attachments; it may contain a virus.
- E-mail is not an entirely secure medium and should not normally be used for sensitive or confidential information.

<u>Contact with Children Outside of School Hours</u>

Increasingly staff and students alike are encouraged to personalise learning with the use of technologies and contact extending beyond the traditional classroom. This contact often involves the use of e-mail as well as forums and chat rooms hosted on school Virtual Learning Environments (VLEs)(ClassDojo)

Staff should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role. Staff should ensure that all communications are transparent and open to scrutiny.

Staff should limit contact with young people to official channels of communication. Email contact with students is limited entirely to the message system provided by the ClassDojo. Other school accounts should not be used without the express permission of the e-safety officer and private accounts should never be used under any circumstances.

Staff should also take great care in the use of nicknames or automatic signatures.

In terms of exchanges on forums/blogs/chat these communications should be limited to school based, open, transparent and logged locations such as the school VLE.

Staff should not use their private mobile phones as a method of communication with students at any time without specific consent and knowledge of the school senior management team. This includes giving their personal home or mobile phone numbers to pupils to allow those pupils to contact them. Even then this contact should be for only clearly defined purposes agreed by senior management.

Social-networking sites

For their own protection and that of the children, staff working in the school must not accept requests from children to be included in their personal online activity (eg on facebook or other social networking sites) Staff must also not request these online relationships with children in the school.

Staff are advised not to show comments or any other posts relating to any person or organisation with whom you share a professional relationship. This includes children, parents, governors and work colleagues.

Staff are advised to consider carefully accepting or requesting online social networking with children who have left the school.

Staff should be aware that social networking with parents or carers of pupils may result in their personal details being made available to the pupils and the wider community.

Digital Images

Staff are advised to use the school equipment to record and store digital images.

Where possible, all images should be uploaded and stored securely on the school server as soon as possible after they have been created.

Images must not be stored temporarily on mobile storage devices or on computer hard-drives where these will be removed from the school premises.

Where images are stored on temporary devices, they should be uploaded as soon as possible and deleted from the device immediately.

Internet use in the classroom

Websites used in the classroom should be checked for suitability using the school network.

Children need to be supervised by a teacher or other member of staff when they use internet.

If inappropriate material is discovered by accident, then turn off the monitor or close lid, reassure, report the complete URL to a member of the senior leadership team.

Use of school laptops outside of school

Personal use of technology by staff is allowed, including use at home. Staff should ensure that they have absolute control of a school laptop and its use when it is allocated to them. Each member of staff must remember that for a “third party” to use a school laptop in their home, they would either need to be:

1. Logged on by the member of staff responsible for the laptop

2. Provided with the confidential log in details by the member of staff responsible for the laptop

Therefore, staff should be aware of, and take all reasonable steps to ensure that the following risks are avoided:

- Access to confidential information stored on the laptop or peripheral devices by family members or friends.

- Access to inappropriate online material by family members using the school equipment

Staff must ensure that no data or images relating to children is stored on their laptop, thereby presenting risk that confidential information or images may be viewed or used by third parties.

If confidential data or images of children are required for legitimate work, these must be stored and accessed using the Central Hosting Network via the use of a 'Key Fob'. These will be provided to all staff who will require access to school files out of the school premises.

Inappropriate and Illegal Material/Content

Some types of Internet material or content are considered inappropriate for staff to be accessing. It is a criminal offence to access/create/save some types of information from the Internet.
Clearly all staff should not view, download or create inappropriate, illegal or criminal content. Any member of staff that does so should be aware that the sanctions that can be applied range from disciplinary to criminal. Access to the Internet in schools is always logged and can be monitored or retrospectively investigated.
As a result staff should be alert to the possibility of accessing inappropriate and illegal material and take steps to avoid this. Staff should avoid creating material that could result in civil or criminal action.

Any activity that is illegal would be a breach of civil law and could result in, upon conviction, having to pay damages / compensation to an individual or organization that brought a case to court.

Any activity that is a criminal offence, if proven in court, would lead to a criminal record and possible fines or imprisonment.

The range of behaviours is clearly huge and cannot possibly be covered completely in this guidance but some could be so serious as to constitute gross misconduct.

Examples of inappropriate behaviour include but are not limited to:

• Attempting to access adult pornography of any type on school computers.

• Making indecent, offensive or threatening comments about pupils or colleagues on social networking sites. (Potentially a criminal offence under Protection from Harassment Act 1997)

• Contacting pupils by email or social networking without prior senior management approval.

• Trading in sexual aids, fetish equipment or adult pornography.

I have read this Acceptable Use Policy and agree to abide by the guidance within it.

Things staff should do	Things staff should not do
Use the school network for school-related purposes only. Ensure that pupils abide by their own AUP for the use of networked resources. Report immediately any misuse of resources or unsuitable material to the named E-safety officer (J McCrossan) Ensure the confidentiality of passwords for any device or any website (including your VLE) to anyone else. Be responsible for ICT equipment and ensure that it is locked away or by other means secure when not in use. Check out websites, in school, before using them with a class. Follow the school policy on keeping personal information about children that you need to take away from school secure. Consider the content that is displayed on social networking sites and ensure that it does not call yourself or the school into question. Ensure that parental permission has been granted to display images of pupils publicly Use the secure centally hosted network to access pupil data and images outside of school	Give personal e-mail addresses or phone numbers to young people. Accept students as “friends” on social media accounts. Use a personal camera or phone to capture images of children. Use personal computer equipment to process images of students at home. Engage in electronic contact with students beyond your professional duties and beyond “normal working hours” for your role. Behave inappropriately on the Internet. Examples of this can be found in the “Inappropriate and Illegal Material/Content” section. Store personal data/images about pupils on temporary storage devices or on the hard drive of a laptop where these will be removed from the school premises.

I have read this Acceptable Use Policy and agree to abide by the guidance within it.

I understand that sanctions for the misuse of the internet and other networked resources range from disciplinary to criminal.

Name:_____

Date:_____

Signature:_____