# Safe & Responsible Use of ICT Policy

This policy is in line with the Ethos and Values of
Blackburn Central High School

## Document Control

This policy has been approved for operation within Blackburn Central High School

| | |
|---|---|
| Date approved | September 2014 |
| Date of next review | September 2016 |
| Review period | 2 Years |
| Policy status | Statutory |
| Owner | NCH |

Blackburn Central High School
striving for outstanding

Headteacher
Mrs. D Atkinson
Haslingden Road
Blackburn BB2 3HJ

tel. 01254 505 700
fax. 01254 505 701
eml. info@bchs.co.uk

web. www.bchs.co.uk
@BCHS_uk
BCHS with Crosshill

# Safe and Responsible Use of ICT Policy

## 1 Introduction

Blackburn Central High School with Crosshill (BCHS) is committed to protecting pupils, employees, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

The school, supported by the central ICT team within Blackburn with Darwen (BwD) local authority, will take appropriate steps to protect the ICT equipment, systems and data from threats, including but not limited to unauthorised access, computer viruses, violation of privacy and interruption to service.

### 1.1 Expectations

This policy applies to all users of BCHS ICT equipment, systems and data (for definitions, see Appendix 2) and must be adhered to at all times.

All school staff have a responsibility to familiarise themselves with this policy before using the BCHS ICT equipment and systems. Each staff user must read, understand and sign to verify they have read and accepted this policy (see appendix 1).

The appropriate Responsible Use Agreement (RUA) form should be signed by all staff and pupils, and a parent or guardian of each pupil. A signed RUA form should be returned before a user is permitted access to BSF ICT services. Signed RUAs will be stored safely for future reference by the school.

Any user found to have breached the terms of this policy may be subject to the school disciplinary procedure. There may be occasions when the police must be contacted (See appendix 14). Early contact should be made by the Headteacher or SLT ICT lead to establish the legal position and discuss strategies.

### 1.2 Purpose

The purpose of this policy is to:

- Define the acceptable use of BCHS ICT equipment, systems and data
- Ensure all use of ICT equipment, systems and data is legal, ethical, and consistent with the aims, values and objectives of BCHS.
- Inform all users of their personal responsibilities when using the BCHS ICT equipment, systems and data.
- To protect the BCHS ICT equipment, systems and data from all threats whether internal or external.
- To ensure that those who use the BCHS ICT equipment, systems and data are aware of the requirements of IT Security and Acceptable Use.
- To ensure that those who use the BCHS ICT equipment, systems and data are aware of their roles and responsibilities in applying, enforcing and complying with IT Security and Acceptable Use.

### 1.3 Objectives

The objectives of this policy are to:

(1) create and maintain within the school a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect;

(2) ensure that users are aware of and fully comply with all relevant legislation and guidance around ICT security and safe and acceptable use of ICT;

(3) ensure that ICT equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school.

### 1.4 Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of BCHS ict systems, both in and out of school. It also sets expectations for the appropriate, legal and safe use of all equipment in school, including legacy equipment and devices belonging to staff and pupils.

It also covers:

- All equipment that is owned or leased by BCHS or BWD.
- Guest devices authorized to connect to BCHS ICT systems.

The Education and Inspections Act 2006 empowers the Headteacher, to such an extent as is reasonable, to regulate the behavior of pupils when they are off the school site and empowers members of staff to impose disciplinary sanctions for inappropriate behaviour. This applies to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the BCHS community.

**2 Compliance with policy and standards**.

The ICT equipment and systems is first and foremost provided to enhance, enrich and extend learning for the BCHS community.

**2.1 All users**

All those accessing the BCHS ICT equipment and systems, whether pupils, staff, or those managing it, will comply fully with the acceptable use policies and adopt the prescribed standards, including:

- compliance with all current legislation in England such as the data Protection Act 1984 (to protect personal data), the Computer Misuse Act 1990 (to deter hacking) and the Copyright 1988 (to stop illegal copying of software) (Appendix 6);
- compliance with and adoption of the agreed password standards (Appendix 2)
- adoption of safe practices to ensure the integrity of the ICT equipment and systems, password security and data security.
- compliance with the appropriate reporting mechanisms should they suspect an account has been compromised, ICT security breached or safeguarding issues arise.

The BSF IT Systems are provided primarily for the purpose of conducting and supporting learning and teaching activities; however personal usage is permitted as long as that does not:

- take place during lesson time or otherwise interfere with the user's professional role;
- bring the BCHS community into disrepute.

All BCHS users should be aware that usage may be monitored and/or recorded.

**2.2 BCHS staff**

In general, the acceptable use standard for school staff is the same as for pupils except:

- it is acceptable for a member of the school staff to access and use one of their pupils' personal accounts, in order to assist the pupil in using the BCHS ICT equipment and systems;
- in some circumstances (e.g. where work has been completed but not submitted and a pupil is unavailable) it is acceptable for a member of the school staff to access a pupil's files;
- a pupil's work may be altered by an appropriate member of the school staff, if this is done visibly, and for the purpose of marking and correcting the work.
- members of the school staff should not alter a pupil's work in such a way that the corrected file appears to be the pupil's own work.
- members of the school staff should not use any other users ICT Service user account login for work or personal matters.

**2.3 Temporary users**

All temporary users will be required to:

- sign the acceptable use agreement and agree to abide by the requirements set out in this policy;

**2.4 Operations Staff and Authority Staff**

ICT operations staff and Authority staff may have access to other users' information and files within the BCHS ICT equipment and systems. This information will only be accessed for operational purposes. It must never be copied outside the BCHS ICT equipment and systems. Inappropriate access to, or misuse of, personal information within the BCHS ICT equipment and systems will be considered a disciplinary offence.

## 3 ICT Security

A number of different groups have responsibility within BCHS ICT for aspects of ICT Security.

### 3.1 Governing Body Responsibilities

The governing body has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. The day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

### 3.2 Headteacher Responsibilities

The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's AUP/ICT Security Policy is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.

The Headteacher, in accordance with the School's Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained and all items accounted for at least annually. This asset register will be maintained by the school's IT support team.

The Headteacher is also responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:-

- registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data;
- registrations are observed with the school;
- BCHS has a current Data Protection Policy, defining how categories of information are assessed and recorded.

In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and that the appropriate controls are in place for staff to comply with the Policy. The Headteacher or Chair of Governors should ensure that details of any suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

### 3.3 BwD LA Internal Audit responsibilities

The Internal Audit Section of Blackburn with Darwen is responsible for checking periodically that the measures prescribed in each school's approved ICT Security Policy/AUP are complied with, and for investigating any suspected or actual breaches of ICT security.

Specialist advice and information on ICT security may be obtained from the Education ICT Group, who will liaise with Internal Audit on such matters.

### 3.4 School Responsibilities

The governing body and Headteacher are ultimately responsible for all school responsibilities.

The school is responsible for:

- Ensuring appropriate arrangements are applied for the removal of any ICT equipment from its normal location, unless part of managed service activities. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- Giving adequate consideration to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be allowed access to the school's server or servers that provide access to data.
- Defining and documenting the requisite level of protection for data and documents according to the information classification system.
- Defining and documenting appropriate levels of access to the network and associated resources including the Learning Platform and Information Management System (SIMS).
- Ensuring the Ethical and safe disposal of decommissioned equipment not covered by the managed service
- Ensuring the Integrity of data, both during repair of faulty equipment and the disposal of assets not covered through the managed service.

### 3.5 User accounts

Access to the equipment and systems will be by individual user account. All users will be required to comply with minimum password standards appropriate to the user group (appendix 3).

- It is the school's responsibility to ensure that enabled user accounts are available only for current staff and pupils and that IT support team are informed of accounts to be disabled.
- The user account of anyone who is under investigation for inappropriate use of the system must be disabled promptly.
- IT SUPPORT TEAM may generate test accounts for the purpose of technical systems monitoring; however no other user accounts should be created for fictitious staff or pupils.

Access to another user's data may be given in exceptional circumstances. Should this be required users should seek advice from the Headteacher and IT SUPPORT TEAM.

### 3.6 All users responsibilities

All users of the school's ICT systems and data must comply with the requirements of this Acceptable Use Policy, which are summarised in *Acceptable Use Agreement'* (see Appendix 1).

All users are responsible for:

- the use of their unique logon details (username and password) and email address and for all content that is transmitted, received and stored by their user account; **your password and access to your account must remain protected at all times** – ***passwords must not be shared with other users (staff or pupils)***;
- reporting concerns over password security immediately;
- notifying the Headteacher of any suspected or actual breach of ICT security (where the level of breach requires it, the Headteacher should inform Internal Audit);
- looking after all computer equipment, ensuring they leave PCs and peripherals in the condition in which they were found;
- ensuring any mobile devices used in school are, when not in use, switched off fully, connected for charging and stored in a secure place;
- endeavouring to protect Blackburn with Darwen Bolton BSF equipment and the equipment and systems or network against Viruses, Malware, Zero Data Attacks and other forms of software based attacks;
- reporting any inappropriate use of BSF ICT services (see section 7);
- following the ICT Asset Protocol when taking any school ICT equipment off the schools premises.

Users should not make any attempt to disable or reconfigure any ICT security measures or software on ICT equipment, including Anti-virus software or seek to bypass any monitoring, filtering or security measures that are in place.

### 3.7 Staff users additional responsibilities

Staff users are responsible for;

- Protecting access to their account wherever the account is accessed and for maintaining the appropriate confidentiality of their data, observing the following precautions when accessing sensitive or confidential data :-
    - devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information.
    - users must not leave computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
    - following a 'clear desk policy', i.e. hard copies of sensitive data are not left unattended on desks;
- Adhering strictly to the protocol for protecting data stored on removable media and mobile devices, including adoption of secure passwords
- Following the security aspects of the protocols for using both fixed (in timetabled or bookable ICT suites) and mobile devices.
- Ensuring pupils in their care are reminded regularly of expectations around appropriate use of BSF equipment and systems, ICT security and E-Safety
- Returning portable equipment signed out to them for updates when requested to do so.

### 3.8 BSF ICT service provider

BSF Service provider employees or contractors have responsibility for:

- Ensuring all data held on the managed service network is backed up. This process meets the Government Baseline security criteria.
- The configuration, operation and on-site support of all BCHS ICT services. Within the context of security they are responsible for bringing any security incidents, either perceived or actual, to the attention of the Client Delivery Manager and Security & Continuity Manager.
- Day to day management of the Managed Service ICT equipment, systems and data including responsibility for controlling access to these assets.
- Administering the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.
- ethical and safe disposal of decommissioned equipment covered by the managed service
- Integrity of data during both repair of faulty and disposal of equipment covered through the managed service.
- measures to guard against unauthorised access to data, such as ensuring that all data is held in a secure location.
- Ensuring approved security patches and service packs are in place on all devices.

## 4 Online communication and use of the web to download/ upload information

### 4.1 Provision of internet access and email

**Internet access**

The provision of the Internet access is owned by the Council and all access is recorded and logged.

Users browse the Internet through a filtered service that is designed to reduce the risk of access to inappropriate material. Nevertheless this filtering cannot be 100% effective, and users should be aware of the possibility of access to inappropriate material and know what to do if such material is displayed (See appendices 13 and 14). This service is currently provided by BwD and the school's software application call WebSense.

Where a user's job role requires them to access inappropriate or restricted sites, a written approval must be obtained from the head teacher prior to access, and advice sought from the LA ICT team.

The ICT systems provides facilities for publication on the World-Wide Web for school-related information. The BSF Learning Platform also provides users with tools to communicate across the school community and to upload and publish ideas and resources.

**Email**

All users will be provided with individual email accounts and are able to use these for communication with other pupils and staff, both within their own school and with other schools. When the facility is available, this system will be managed by the school to ensure access is appropriate to the school's requirements.

Email to and from the Internet is permitted, but pupils should receive E-Safety education before using the system (Please see our E-Safety Policy). It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 (see Appendix 2) and the Freedom of Information Act 2000. Email use is filtered and can be recorded.

### 4.2 Guidance on use

All use of electronic forms of communication or use of the web to share, access, download or publish information, should:

- Ensure that personal and financial information is safeguarded, including personal contact details.
- Ensure the security of the ICT network by maintaining up to date virus protection and following links downloading files from reliable sources only.
- Always use their 'learning futures' or 'blackburn.gov' email addresses when sending, receiving or forwarding emails containing RESTRICTED information.
- Access news groups, bulleted boards and other similar communication groups for educational purposes or those relating specifically to their professional role only.

- Use social networking sites, real time chat, discussion forums, online games and other similar web resources only when expressly permitted to do so for educational purposes, or as part of a member of staff's professional role.
- Only publish information they have permission to use from the school and individuals
- Abide by copyright laws and licensing constraints regarding the use of software and electronic media.

Use of electronic forms of communication or web access to share, download or publish information, for the following purposes is not permitted and may result in disciplinary and legal action where necessary:

- Sending, receiving, accessing or downloading obscene, racist, or insulting language, images, video or other media.
- Sending, receiving, accessing or downloading content in any form, containing provocative, suggestive or discriminatory language.
- Engaging in activities that bully, harass, mislead others or cause distress to groups or individuals.
- Accessing sites that are violent, hateful and discriminatory, promote hacking, or encourage gambling.
- Revealing information of a personal or private nature, or information that may lead to identification of an individual.
- Sending SPAM
- Downloading, uploading sharing or copying any content of copyrighted material, unless permission has been sought and given by the owner of the copyright (Please note breaching this is a criminal act and may lead to personal prosecution).
- Forwarding emails or information containing personal, confidential or sensitive information (therefore classified as PROTECT or RESTRICTED information - see Information Classifications Section) from the BSF learning futures or Blackburn.gov/Bolton.gov to any personal email addresses including the employee's own personal email.
- Sending or forwarding emails containing RESTRICTED information to recipients outside the school who do not have 'blackburn.gov' email accounts. *This should be done through your standard school email address with appropriate encryption. Contact the BT&IT*
- Using the LA and BCHS IT Systems to support private business or money making activities.

Any use that may potentially bring the users, the school and or the local authority into disrepute. (where a user is unsure whether a particular use is acceptable, it is the users responsibility to consult the SLT ICT lead and IT SUPPORT TEAM).

**5 Dealing with incidents of inappropriate or illegal misuse.**

It is expected that all members of the BCHS community will be responsible users of ICT, following the principles in this policy. However, there may be times when infringements of the policy take place, through careless or irresponsible misuse, or occasionally, through deliberate misuse.

**5.1 Providing evidence of user activities - Systems Monitoring**

All users should be aware that in order to provide safe and secure systems the following security controls are in place:

- Email systems are filtered and recorded
- Web usage is actively filtered and recorded
- System usage is recorded
- System files, etc. may be accessed to ensure confidentiality, integrity and availability.
- All BCHS and LA ICT services are monitored and audited, including using automated alerting systems. **Logs can and will be retrieved after an incident has occurred**.
- Any school user data retained by filtering systems will not be released unless authorisation has been given by the Headteacher or the SLT ICT lead.
- Checks will be carried out to identify violations such as placing rogue equipment or software on the network or systems.

**5.2 Responding to ICT misuse**

**Inappropriate misuse**

It is most likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a **proportionate** and consistent manner through

- the normal Behaviour for Learning procedures for pupils (see Appendix 13)
- agreed school disciplinary procedures for staff,

and that members of the school community are aware that incidents have been dealt with.

If members of staff suspect that misuse might have taken place (but not illegal) the incident can be investigated by MLs or PPCs as appropriate, with the support of IT SUPPORT TEAM technicians, ensuring that evidence is preserved and those carrying out the investigation are protected.

**Illegal misuse**

Illegal activities involving use of ICT include ;

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist or extremist material
- other criminal conduct, activity or materials

If a member of staff suspects a user of illegal misuse or actually finds evidence of illegal activities, the flow chart of responses and actions must be followed (see appendix 14), in particular the sections on reporting the incident to our school IT support team, the Police and the preservation of evidence.

**Security incidents**

IT SUPPORT TEAM will appoint the Security & Continuity Manager and the authority representative should instigate an investigation of any security incident, with a view to determining the appropriate actions to take as a result of the incident.

The investigation should, wherever possible, determine the extent of an incident, the impact of the incident, and the source of the incident. It may not always be possible to complete such investigations, but an attempt should be made to get far enough to make a reasonable recommendation as to actions that should be taken as a result of the incident. Where a security incident affects ICT systems the Client Delivery Manager should exchange appropriate information with the Authority, in order to coordinate the resulting actions. This notification should take place at the earliest appropriate time.

It is particularly important that all security and E-Safety incidents are logged and that a detailed record is kept of the investigation and resultant actions. The Client Delivery Manager is responsible for this log, even though other people will carry out specific parts of the investigation and resultant actions. Reports should be submitted to the Authority for review or further investigation.

All security incident reports and logs must remain confidential and only authorised personnel will be permitted to view this material.

The local law enforcement agency will be contacted if the severity of a security breach necessitates this course of action under advice and guidance from the IT SUPPORT TEAM Security and Continuity Manager.

Investigations are normally conducted for all security incidents including but not limited to the following:

- Unauthorised access or an attempt to access a resource or other users account without approval.
- Unauthorised modification to systems whether successful or unsuccessful.
- Unauthorised disclosure of school information.
- Deliberate or unintentional hacking attempts such as Denial of Service attacks, etc.
- Rogue software or hardware appearing on the **BCHS** network.

**6 Policy review**

This policy will be reviewed by the SLT ICT lead, DoL ICT and IT SUPPORT TEAM annually.

Due to the rapidly changing nature of technology, this policy may be updated more regularly as a result of advice from the LA. Any changes should be shared with staff at the earliest possible opportunity.

**Appendix 1 BCHS with Crosshill Responsible Use Agreement**

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this agreement. Staff should consult the school's Safe and Responsible Use Policy for further information and clarification.**

- I will promote e-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.
- ICT equipment and software are the property of the school/Local Authority and I understand that it may be a criminal offence to use it for a purpose not permitted by its owner.
- I will ensure that my use of technology will always be compatible with my professional role.
- I understand that I am responsible for my own use of new technologies, and will ensure that I technology safely, responsibly and legally.
- I understand that school and personal ICT equipment may be used for private purposes out of school directed time only and that the use of school equipment may be monitored and should be in keeping with my professional status
- I understand that I must not use school ICT resources for personal financial gain, gambling, political purposes or advertising.
- I understand that my information systems and Internet use is subject to filtering and as such may be recorded.
- I understand that it is my duty to protect my passwords and personal network login and should log off the network or lock the device before leaving it unattended.
- I will not install any software or hardware without permission.
- I understand my personal responsibility for safeguarding and protection of data and will comply with the data protection Act of 1998 and any other legal, statutory or contractual obligations that the school and LA inform me are relevant
- I will familiarise myself with the public sector information classification framework. This national Protective Marking System classifies information in the following three levels of classification: unclassified, protect and restricted.
- A pupil's work may be altered by an appropriate member of the school staff, if this is done visibly, and for the purpose of marking and correcting the work but it is unacceptable that a member of the school staff alters a pupil's work in such a way that the corrected file appears to be the pupil's own work.
- I will report any known misuses of technology, including the unacceptable behaviour of others to the SLT ICT lead and IT support Helpdesk who will in turn escalate relevant incidents to the Client Delivery Manager for investigation.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safeguarding to the designated senior person responsible for child protection.
- I will report any incidents of concern regarding suspected or actual failure of technical safeguards to the school Child Protection Officer, the SLT ICT lead and IT SUPPORT TEAM.
- I will ensure that any electronic communications with pupils are appropriate to my professional role.
- I will ensure that all electronic communications are written in a professional manner and understand that they are potentially public property.
- I understand that it is my duty to respect technical safeguards in place and will not attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services.
- I will take reasonable precautions to prevent damage to or loss of ICT equipment in my charge, adhering to protocols for using mobile and fixed devices with pupils and ICT assets.

The school may exercise its right to record and monitor the use of the school's technology, including Internet access and email. The school will take the necessary action 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 have read, understood and will abide by the BCHS with Crosshill Responsible Use Policy.**
- Signed: …… Capitals: ……..…… Date: ……
- Accepted for school: ……. Capitals: ……..…….

**Appendix 2 : BCHS Pupil Safe and Responsible Use of ICT Policy Agreement**

**School Policy**

New technologies have become integral to the lives of young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people have an entitlement to safe internet access at all times.

This Safe and Responsible Use Policy is intended to ensure:

- that young people will be r**esponsible users and stay safe** while using the internet and other communications technologies for educational, personal and recreational use.
- that school **ICT systems and users are protected from accidental or deliberate misuse** that could put the security of the systems and users at risk.

The school will try to ensure that all pupils will have good access to ICT to enhance their learning and, in return, expects pupils to agree to be responsible users.

**Safe and Acceptable Use Policy Agreement**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for file sharing unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Safe and Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include : loss of access to the school network / internet, catch-ups, Remove, suspensions (PPA), contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Responsible Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.**

**BCHS Pupil Safe and Responsible Use of ICT Agreement Form**

This form relates to the pupil Safe and Responsible Use Policy (SRUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Responsible Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil : ……..…….. Learning group : ……..

Signed : …… Date : ……

**Appendix 3 : ICT Code of Conduct**

Be a safe and responsible user.

- Treat your password like your toothbrush – do not share it with anyone
- If you think someone else knows your password, report it to a member of staff as soon as possible
- Do not try to use any other person's username or password
- Save your work often (perhaps after every couple of minutes)
- When printing, make sure that you have checked for mistakes carefully on the screen first
- Avoid sending too much information to the printer – print only what you really need
- Food and drink, including chewing gum, are not allowed in the ICT areas
- Report any technical problems to the teacher
- Stay away from cables/wires behind the computers
- Check everything is left tidy for the next user

Do **not** do any of the following:

- Use a chatroom without permission
- Browse the internet when you have not been allowed
- Play games (the website will be blocked by NetSupport)
- Look at obscene or offensive material
- Download or stream video or music files without permission
- Check e-mail without permission
- Produce offensive material

**Treat all equipment with care as you would not appreciate having to pay a repair bill!**

**Appendix 4 :** Definitions of ICT systems

For the purposes of this document the terms 'ICT' or 'ICT equipment', 'ICT systems', 'ICT data' and 'ICT user' are defined as follows:-

- 'ICT' (or 'ICT equipment') means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, stand-alone, network or attached to a mainframe computer), workstation, word-processing system, desk top publishing system, office automation system, messaging system, any other similar device and peripherals for these devices;
- ICT system means any virtual, online or networked resource or facility available through the ICT managed service.
- 'ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound; see appendices 4 and 5
- 'ICT user' applies to any member of school staff, pupil or other authorised person who uses the school's ICT equipment, systems and/or data.

**Appendix 5:** Password security guidance

**Password Policy - Strong**

| Attribute | Strong |
|---|---|
| Password History Length | 10 |
| Password Complexity Status | TRUE |
| Minimum Password Length | 7 Characters |
| Minimum Password Age | 0 days |
| Maximum Password Age | 60 days |
| Lockout Threshold | 5 invalid logon attempts |
| Lockout Observation Window | 30 minutes |
| Lockout Duration | 30 minutes |

**Composition**

This policy would require the user to have at least a 7 digit password made up of a combination of character types. Passwords cannot be the same as the previous 10 passwords.

The password will expire after 60 days.

The account will lockout after 5 invalid attempts, but will automatically unlock after 30 minutes.

**Security**

This is the most difficult to use but in terms of security this policy is the strongest as the risk for unauthorised access to user accounts is minimal.

**Recommendations**

As this is the most secure policy it is recommended that this is applied to users that have access to additional sensitive data or have additional privileges:

- Teachers
- Staff

**Password Policy - Fair**

| Attribute | Strong |
|---|---|
| Password History Length | 5 |
| Password Complexity Status | FALSE |
| Minimum Password Length | 5 Characters |
| Minimum Password Age | 0 days |
| Maximum Password Age | 365 days |
| Lockout Threshold | 5 invalid logon attempts |
| Lockout Observation Window | 30 minutes |
| Lockout Duration | 30 minutes |

**Composition**

This policy would require the user to have at least a 5 digit password made up of any characters. This cannot be the same as the previous 5 passwords.

The password will expire after a year.

The account will lockout after 5 invalid attempts, but will automatically unlock after 30 minutes.

**Security**

This is fairly simple to use and in terms of security this policy is fair/moderate, as the risk is lower for unauthorised access to user accounts.

**Recommendations**

As this is not a high security risk policy and not too complex to use it is recommended that this policy is applied to:

- Pupils (Non SEN)
- Parents
- Visitors

**Password Policy - Weak**

| Attribute | Strong |
|---|---|
| Password History Length | 5 |
| Password Complexity Status | FALSE |
| Minimum Password Length | 5 Characters |
| Minimum Password Age | 0 days |
| Maximum Password Age | 365 days |
| Lockout Threshold | 5 invalid logon attempts |
| Lockout Observation Window | 30 minutes |
| Lockout Duration | 30 minutes |

**Composition**

This policy would require the user to have at least a 4 digit password made up of any characters and can be the same as any previous passwords.

The password does not expire and does not lockout if entered incorrectly.

**Security**

Although this policy is easy to use, in terms of security this policy is weak, as there is a high risk of unauthorised access to user accounts, due to the simplicity of the structure.

**Recommendations**

Due to the high security risk it is recommended that this policy is applied to SEN pupils only. But if required can be applied to any user.

**General expectations:**

- Use a strong password and keep it confidential. Never write your password down or store it in a computer system.
- Never reveal your passwords to anyone (includes colleagues, BT&IT Service Desk, Line Managers, family and friends)
- Never use the 'remember password' function.
- All users must prevent their username and password being used to gain unauthorised access to Blackburn with Darwen Bolton BSF equipment and equipment and systems by locking the workstation when it is not in use so that casual overlooking and unauthorised tampering is prevented (for guidance on how to lock your screen***name***).
- If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the IT SUPPORT TEAM service desk.

- Only use the user account to store data that is associated with the school.
- Users must not divulge their account passwords to others, must not permit others to use their accounts, and must not use accounts intended for the sole use of other individuals.
- Lock the workstation when it is not in use and log off when leaving the room unattended.
- It is wise to save work before locking the workstation.
- Do not attempt to use your colleague's credentials.

**Appendix 6: Using mobile devices with students**

All mobile devices are the property of the school and must be treated as such. Mobile devices at BCHS include laptops, netbooks, iPads and iPod touches.

Mobile devices **must** be locked away whenever they are not in use.

Mobile devices are not covered by insurance if a device is :

- left unattended in an open classroom
- left in a classroom or office and not securely locked away overnight
- left on in a bag (e.g. laptop in laptop bag) and overheats

Replacement costs for loss or damage would lie with the department or faculty of the member of staff responsible for the device when it was damaged or went missing.

**Responsibilities**

- The DoL is responsible for booking out the mobile devices in the lapsafes / secure storage boxes in their area.
- All staff must complete a separate user record sheet in the security and maintenance folder with each lapsafe / secure storage **every session** in which they lend out mobile devices to pupils showing :
    - Name of member of staff
    - Date and time (period)
    - Which pupils used which device
    - Any problems with the device
- All staff must notify the IT Support Helpdesk of any problems with, damage to, or loss of mobile devices as soon as is practicable.
- Staff must ensure pupils use the device from the same shelf / slot in the lapsafe / secure box (which should usually mean the same device, unless a machine has been 'hot swapped' by the school IT support engineers) – this should reduce log in times as well as improving pupil accountability.
- Pupils are responsible for the device they are using – pupils must carry out a visual check (of screen and keyboard) that the device is not damaged before using the machine and report any issues to the member of staff.

The SLT ICT lead will upload an individual asset register for each lapsafe and secure storage box. Printed copies of these User Record Sheets will be placed in the Security and Maintenance folder with each storage unit. In addition to the user details provided by staff, the User Record Sheet should provide the following information :

- Name and location of lapsafe / secure storage
- Shelf / slot number of each device
- NetSupport group
- Serial number of device

Staff can either write the pupil's names next to the shelf / slot number each time they use a lapsafe, or download the file, paste in the pupils' names from a marksheet (so they do not have to write them out each lesson), and place a print off in the MS folder when they use one or more of the devices.

**NetSupport and networked devices**

The use of networked mobile devices (laptops and netbooks) by pupils during class should be monitored by staff using NetSupport.

Laptops and netbooks are configured individually to a group (a-d) within a particular lapsafe so that they can be used with the NetSupport software. Each device **must** therefore be returned to the **same shelf** in a lapsafe from which it was taken.

**Mobile device protocol**

Giving out devices.

1. Collect the storage unit key from the DoL (or designated person).
2. Check the previous User Record Sheets to see if any devices are missing, damaged or not working and rearrange groups accordingly.
3. Note any devices that are missing and when practicable send a report to our school IT support team and the DoL.
4. Complete your class details on the User Record Sheet.
5. Hand out the devices (pupils should only collect them from the storage unit under the strictest supervision – damage to cables must be avoided or the department will have to pay for repairs).
6. Pupils carry out a visual check of the devices – record damage.
7. Pupils log on when ready – please email the our school IT support team helpdesk if a pupil is having problems logging on.

   (Note – staff should know how to change pupil passwords using the widget on the N-able learning platform.)

Collecting devices back in.

1. Pupils shut down the device.
2. Carry out a visual check of the devices as the pupils return them – note any damage, and when practicable send a report to our school IT support team and the DoL.
3. Return each device to the correct shelf / slot and re-connect the power supply (pupils should only do this under the strictest supervision – the correct state of the lapsafe / storage device is the responsibility of the teacher).
4. Carry out a final count of the devices, and then lock the storage unit.
5. Return the key and the unit to the DoL (or designated person).

**Appendix 7:** Use of fixed devices in bookable ICT rich spaces

Replacement costs for loss or damage would lie with the department or faculty of the member of staff responsible for the device when it was damaged or peripherals (mouse / keyboard / microphone / headphones) went missing.

**Responsibilities**

- The DoL is responsible for booking out some / all the fixed devices.
- All staff must complete a separate user record sheet (seating plan) in the security and maintenance folder for the space **every session** in which they use the fixed devices showing :
    - Name of member of staff
    - Date and time (period)
    - Which pupils used which device (seating plan of workstations)
    - Any problems with the device
- At the end of the session staff should -
    - check each workstation has all the correct equipment in the same condition as when they entered the room.
    - pass the completed user record sheet to the relevant DoL.
- All staff must notify the our school IT support team helpdesk of any problems with or damage to the device and its peripherals, or loss of peripherals, as soon as is practicable.
- Staff must ensure pupils use the device in the same workstation (which should usually mean the same device, unless a machine has been 'hot swapped' by our school IT support team technicians) – this should reduce log in times as well as improving pupil accountability.
- Pupils are responsible for the device they are using – pupils must carry out a visual check (of screen, keyboard and mouse) to check that the device is not damaged before use and report any issues to the member of staff.

The SLT ICT lead will upload an individual asset register for each ICT rich space. Printed copies of these User Record Sating plans will be placed in the Security and Maintenance folder with each storage unit. In addition to the user details provided by staff, the User Record Sheet (Seating plan) should provide the following information :

- Name and location of ICT rich space
- Workstation location
- Serial number of device

**NetSupport and networked devices**

The use of fixed PCs (both thick and thin client) by pupils during class should be monitored by staff using NetSupport.

**Appendix 8:** ICT Asset Protocol

1. Where any ICT Asset (any school ICT equipment) is taken outside the Site it shall be checked out by the DoL upon leaving the Site and checked in upon return using a booking system that requires two signatures at both checking out and returning (see ICT issues record sheet on the next page).

2. Whilst any ICT Asset is outside the Site:

    - the person who checked it out shall be responsible for taking all reasonable precautions and care of it and for its safe return;
    - it shall not be left unattended in any place or vehicle (whether locked or unlocked) other than the residence of the person who checked it out;
    - it shall not be used where there is any material risk of damage from liquids, impact or otherwise;
    - it shall not be lent or entrusted to any other person;
    - Any alleged theft shall be reported to the police and a crime reference number obtained and until the number is obtained it shall be deemed to be a loss rather than a theft.

3. In using any ICT Asset:

    - users shall not attempt to modify or circumvent any antivirus or other security software;
    - users shall not save any data to the Asset that may cause damage or interference or instability to the Asset or any part of the Asset, including any firmware, operating system or other software.

4. In consultation with the school, any person whom the school IT support team reasonably suspects may be in breach of this protocol may be denied permission to remove ICT Assets from the Site.

5. Users with devices on long term loan are responsible for returning the device to school on a regular basis, to ensure updates are installed.

**BCHS ICT equipment issues record sheet**

This record must be signed and dated by the recipient, and retained by the issuing person.

By signing this document you are acknowledging receipt of the items listed in the equipment details fields below, and acceptance of the conditions for responsible use as outlined in the BCHS policy, in particular Appendix 8 (see reverse of sheet).

Please check the equipment before you sign for it and bring any observations to the attention of the person issuing the equipment.

If you encounter any issues with this equipment during normal use, please contact the school IT support team service desk using either the NSM customer portal widget in N-Able, or sending an email (to BCHS-ITSUPPORT@bchs.co.uk)

| **IT Asset Number** | **Manufacturer** | **Model** | **Ancillary items (e.g. power supply, mouse)** | **Condition on issuing** |
|---|---|---|---|---|
| | | | | |
| | | | | |

Recipient name : …….
Please print

Faculty : …….
Please print

Recipient Signature : …… Date : ……..…….

Issuing Person : …….
Please print

Issuer's Signature : ……..……. Date : ……..…….

**Returning equipment.**

| **IT asset number** | **Date returned** | **Condition on return** | **Issuer's Signature** | **Recipient's signature** |
|---|---|---|---|---|
| | | | | |
| | | | | |

**Appendix 9:** Information Classification

Information classification is a means of standardising the way information is assessed, marked and handled according to how confidential it is. The national Protective Marking System to classify information and has been introduced throughout the public sector as the standard framework to allow the safe and appropriate sharing and protection of information. Please familiarise yourself with the following 3 levels of classification from the Protective Marking System, which are referred to throughout this Policy:

**Unclassified**

UNCLASSIFIED is the lowest level of classification and covers all information which can safely be shared or is already publicly available.

Information is UNCLASSIFIED if:

- It is intentionally publicly available
- Disclosure would not adversely affect any individuals, external organisations or the school e.g. School literature, the school website, press releases, all items of public record.

**Protect**

PROTECT is the first level of sensitive information. Information should be classified as PROTECT if "compromise of information would be likely to affect individuals in an adverse manner."

The PROTECT classification should be used where disclosure would:

- Be likely to affect an individual or a small number of individuals in an adverse manner
- Cause substantial distress to an individual
- Breach proper undertakings to maintain the confidence of information provided by third parties (for example, breach commercial confidence with a supplier to the school).
- Breach statutory restrictions on the disclosure of information.

E.g. documents/emails containing name, address, NI, DOB, commercial terms & conditions.

Most of the sensitive information which the school handles will be at the PROTECT level of classification.

**Restricted**

RESTRICTED is a higher level of classification than PROTECT and is used where "compromise of information would be likely to affect the national interests in an adverse manner".

The RESTRICTED classification should be used where disclosure would:

- Put an individual at significant risk of harm or long-term distress
- Release personal information for 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress (i.e. the release of a large amount of PROTECT classified data relating to individuals).
- Significantly undermine public confidence in the Council or other public body
- Cause widespread disruption to the work of the Council or other local public sector
- Organisation
- Significantly impact the LA and BCHS ability to discharge it's duties under the Civil Contingencies Act

The RESTRICTED classification will apply to a small amount of data which the school handles, primarily relating to highly sensitive information on individual pupils and staff. E.g. documents/emails containing, name, address, NI, DOB, Salary, Pension, Benefit details, investigations, fraud etc.

**Appendix 10:** Installation of Software and storage of data

We use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

**Licenses**

Software license compliance requires all software used within the School is legally licensed, in accordance with the Copyright, Designs and Patents Act 1998.

It is the school's responsibility to ensure that all software on the school ICT network is appropriately licensed.

The school is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations.

To ensure the School is compliant the following rules must be adhered to:

- All software must be purchased with a licence appropriate to its intended use.
- All software to be installed on ICT equipment must be RAG tested by the NSM. This includes all Commercial, Shareware, Freeware, and Public Domain Software.
- The (LA) School expressly prohibits the illegal duplication of software.
- Copying, downloading and storing of copyrighted material (such as music, and photographs from magazines) that is not waivered for educational use on to ICT equipment is strictly prohibited.
- It is the school's responsibility to ensure that software added to all devices and desktops on the ICT systems, including guest devices, is appropriately licensed.

**Please be aware that failure to follow this policy could lead to criminal prosecution.**

**Data Ownership**

Data within the BCHS ICT equipment and systems will be owned by a number of different individuals and organisations.

This Policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to (see BCHS Notice of fair processing of data).

**Appendix 11:** Data Protection and Other Relevant Legislation

## The Legislation

### 11.1 Background

11.1.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of :-

- Data Protection Acts 1984 & 1998;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988

11.1.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

11.1.3 The general requirements arising from these acts are described below.

### 11.2 Data Protection Acts 1984 & 1998

The Data Protection Act exists to regulate the use of computerised information about living individuals and gives rights to individuals about whom personal data is recorded (Data Subjects). They may obtain personal data held about themselves, should be told about the use of personal data and can expect it to be accurate. The act places obligations on those who record and use personal data (Data Users). They must follow sound and proper practices, known as the Data Protection principles. Principle 7 requires that security is in place during the collection, use and storage of personal data.

Any requests to view personal data must be in line with the Data Protection and Access to Information procedures.

11.2.1 To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information. This shows you how to log on to the Information Commissioners Site and pay the necessary £35.00 for registration.

11.2.2 It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

11.2.3 Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

### 11.3 Computer Misuse Act 1990

11.3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:-

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

11.3.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

### 11.4 Copyright, Designs and Patents Act 1988

11.4.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

11.4.2 If an organisation is using illegal copies of software the organisation may face not only a civil suit, but corporate officers and individual employees may have criminal liability. If liability is proven this could lead to an unlimited fine and up to ten years imprisonment per offence.

11.4.3 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

11.4.4 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

**11. 5 The Regulation of Investigatory Powers Act 2000**

The Act specifies that communications may be monitored and recorded for "a legitimate purpose" such as system and employee performance monitoring; detection and prevention of crime; detection of unauthorised use (including unauthorised use by employees; protecting against hackers and viruses; and ensuring the Council is complying with regulatory or self-regulatory practices or procedures relevant to the business.

Monitoring can only be carried out legally if the organization concerned has informed its staff that it is undertaking monitoring for these purposes. The provisions of the RIP Act have been taking into account in the formulation of Council policy relating to email and telephone use as detailed later in this document. Consistent with the LA and BCHS policies for Misconduct and Workplace Harassment and Equal Opportunities, non-adherence to this policy may result in disciplinary action being taken by the Council that may result in dismissal and/or Civil or Criminal Court action.

**Appendix 12:** Inappropriate Use

This section does not provide a complete list of usage and behaviours that are considered inappropriate but it gives some examples of misuse, in order to help all users of the ICT Service to make decisions on unclear areas.

The following activities will always be considered inappropriate use of the BCHS ICT equipment and systems by any user:

- ◊ Development, or deliberate release, of rogue code (i.e. viruses, trojans, etc.).
- ◊ Interference with the work of other users (e.g. altering or copying their work).
- ◊ Grooming.
- ◊ Hacking, probing, scanning or testing the weaknesses of a system within the BCHS ICT equipment and systems, or on the Internet.
- ◊ Unauthorised access to systems. Violating or attempting to violate the security of the network.
- ◊ Actions that bring the school, or the BCHS ICT equipment and systems, into disrepute, or that are likely to do so.
- ◊ Deliberately wasting resources (e.g. unnecessary copying or emailing or very large files).
- ◊ Use of the equipment and systems for personal financial gain.
- ◊ Any illegal activity, including breach of copyright.
- ◊ Attempting to log on using another person's username and password.
- ◊ Making your username and password known to any unauthorised person.
- ◊ Creating or storing offensive, intimidating, insulting or harassing material on the school network.
- ◊ Accessing data not intended for you to access.
- ◊ Attempting to bypass filtering, or to access inappropriate or illegal material – such attempts will be reported to the school authority.
- ◊ Leaving your workstation logged in while unattended.
- ◊ Connecting additional devices to data points on the BSF ICT network without the specific agreement of BSF ICT service provider.
- ◊ Attempting to interfere with services to any user, host or network.
- ◊ Taking any action in order to obtain services to which you are not entitled.
- ◊ Conducting any unlawful or illegal activity.
- ◊ Using the services to create, transmit, distribute or store content that invades the privacy or other personal rights of others.
- ◊ Assisting, encouraging or permitting any persons in engaging in any of the activities described in this section.
- ◊ Sending email messages which result in complaints from the recipient or from the recipient's email provider, or which result in blacklisting of the sender's email address or mail server.
- ◊ Sending email or messages which are excessive and/or intended to harass or annoy others.
- ◊ Sending, or attempting to send, spam of any kind from third-party networks using a return email address that is hosted on the BSF ICT mail servers, or referencing an email address hosted on the BSF ICT mail systems.
- ◊ Failing to observe intellectual property
- ◊ Keeping, accessing or transmitting confidential data about other pupils.
- ◊ Producing documents or emails that contain obscene, offensive, unlawful, intimidating, defamatory, harassing, abusive, fraudulent, or otherwise objectionable content as reasonably determined by the school or authority.
- ◊ Causing technical disturbances to the BSF ICT systems by introducing viruses of any kind.
- ◊ Any use that interferes with, or prevents, another user's permitted use of the equipment and systems.
- ◊ Unauthorised modification or reconfiguration of BCHS ICT systems,
- ◊ Using managed service email or messaging systems to engage in inappropriate or nonprofessional communications between either staff, staff and pupils or pupils
- ◊ Any uses of BSF equipment, school ICT equipment of personal equipment connected to the network, intended to bully or harass others.

**Appendix 13 :** Responding to incidents of pupil misuse of ICT

| Behaviour descriptor for any incident involving mis-use of ICT | SIMS Behaviour type | Interpretation | Add to actions / sanctions |
|---|---|---|---|
| Unauthorised use of mobile phone / mp3 player / digital camera / other handheld device | 1 | Texting / listening | |
| Unauthorised use of mobile phone / mp3 player / digital camera / other handheld device | 2 | Makes / Answers phone call | Remove mobile phone (store securely) |
| Unauthorised use of non-educational sites during lessons e.g. youTube | 2 | | Block internet access (using NetSupport) |
| Unauthorised use of social networking / instant messaging / personal email | 2 | | Block internet access (using NetSupport) |
| Unauthorised use of mobile phone / mp3 player / digital camera / other handheld device | 3 | Takes photographs / records sounds without permission (not threatening or abusive) | Remove mobile phone / digital device (store securely) – only return to parents<br>Remove images / recordings from device |
| Unauthorised downloading or uploading of files (internet) | 3 | | Inform onsite IT support team technicians. |
| Accidentally accessing offensive or pornographic material and failing to report the incident | 3 | | Inform onsite Our school IT support team technicians so site can be blocked. |

| Behaviour descriptor for any incident involving mis-use of ICT | SIMS Behaviour type | Interpretation | Add to actions / sanctions |
|---|---|---|---|
| Unauthorised downloading or uploading of files (USB) | 4 | | Remove pupil from computer or other digital device. |

| | | | |
|---|---|---|---|
| | | | Inform onsite Our school IT support team technicians. |
| Unauthorised downloading or uploading of inappropriate files (internet or USB) | 4 | | Remove pupil from computer or other digital device.<br>Inform onsite Our school IT support team technicians. |
| Allowing others to access school network by sharing username and passwords | 4 | | Change password. |
| Corrupting or destroying the data of other users | 4 | | Block account (Our school IT support team technical request through helpdesk) |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | 4 | | Request log print off (Our school IT support team helpdesk) |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | 4 | | Request log print off (from onsite IT support team helpdesk) |
| Using proxy sites or other means to subvert the school's filtering system | 4 | | Inform onsite IT support team technicians |
| Deliberately accessing or trying to access offensive or pornographic material | 4 ('pornography') | | Remove pupil from device (do not switch off device) and immediately request onsite technician support |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | 4 | | Request log print off (onsite IT support team helpdesk) |

| Behaviour descriptor for any incident involving mis-use of ICT | SIMS Behaviour type | Interpretation | Add to actions / sanctions |
|---|---|---|---|
| Attempting to access or accessing the school network, using another pupil's account | 5 | | Block network account |
| Attempting to access or accessing the school network, | 5 | | Block network account |

| | | | |
|---|---|---|---|
| using the account of a member of staff | | | |
| Unauthorised use of mobile phone / mp3 player / digital camera / other handheld device | 5 | Uploads images / sound recording onto the internet or in any way shares images / recordings made without permission | Hand device to onsite police officer (to view and delete images / recordings)<br>Device to be returned to parents after interview.<br>Device (or similar) must not be brought into school again |
| Sharing / supplying offensive or pornahraphic material | 5 | | Remove pupil from device. Do not switch off device – request onsite police and technicians support immediately. |
| Deliberately accessing or trying to access material that could be considered illegal (see list below* on unsuitable / inappropriate activities). | 5 | | Remove pupil from device. Do not switch off device – request onsite police and technicians support immediately. |

**Appendix 14 – Response to suspected or actual illegal UCT misuse**