Promoting Ambition for Change

TEMPLE LEARNING ACADEMY

E SAFETY POLICY
2016 - 2017

CONTENTS

This policy was adopted by the Governing Body of Temple Learning Academy

1. Introduction

1.1 The aim of this guidance is to inform all staff of best practice around E Safety and draw attention to existing local and national guidance on this subject. It is our responsibility to safeguard young people and protect staff from false accusations of improper conduct so that together we can ultimately maintain the safest possible learning and working environments for learners and staff alike.

1.2 This document has been created in line with national guidance issued by the Department for Children, Schools and Families (DCSF) as well as also drawing information from existing policies issued by Leeds Safeguarding Children Board and Education Leeds. It does not replace or take priority over other advice or codes of conduct issued by Education Leeds or any National Guidance issued by other sources.

SECTION 1 - STAFF

1. Social contact with learners, children or young people

1.1 Staff must not establish or seek to establish social contact with learners, children or young people for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a learner, child or young person seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise his or her professional judgement in making a response and be aware that such social contact could be misconstrued.

1.2 All contact with learners, children or young people should be through appropriate channels at all times. Any communication outside of agreed professional boundaries could be prone to misinterpretation and as a result could put both the employee and young person at risk.

1.3 Staff should not give, nor be required to give, their personal details such as home or mobile phone number, Instant Messenger identities or personal e-mail address to learners, children or young people. Staff should not use any of the above means to contact learners, children or young people without the prior and explicit consent of the senior leadership team. Any member of staff found to be in contact with learners, children or young people through any of the above means, or any other unapproved method, without prior consent could be subject to disciplinary action.

1.4 Internal e-mail and approved contact systems should only be used in accordance with the appropriate school or service Information Security Policy.

1.5 This means that members of staff should:

Always seek approval from senior management for any planned social contact with learners, children or young people for example when it is part of a reward scheme or pastoral care programme.

Advise senior management of any regular social contact they have with a learner, child or young person which may give rise to concern.

Report and record any situation which they feel might compromise the reputation of the organisation or their own professional standing.

2. Social Networking websites

2.1 This also extends to use of Social Networking sites. Members of staff must not have any contact with learners, children or young people through such sites and staff must not add learners, children or young people as friends or respond to requests for friendship from children if asked. If a member of staff suspects that an existing friend is a learner, child or young person, they should take reasonable steps to check the identity of the individual and end the friendship should the suspicions not be put to rest.

2.2 It is recognised that personal access to Social Networking sites outside the work environment is at the discretion of the individual, however, members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

2.3 Secure and suitable strength passwords should be devised and security settings should be applied so access to your profile and the information contained is limited to those explicitly given access.

2.4 Personal profiles on social networking sites and other internet posting forums must not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, Information which is confidential or could put others at risk should not be posted on such public domains. If the material you post or display is considered inappropriate or could be considered to bring your academy or profession into disrepute, disciplinary action may be considered.

2.5 For further guidance on social contact with children please refer to LSCB website and Education Leeds Safer Working Practice guidance document.

3. Inappropriate material

3.1 When considering what is defined as inappropriate material it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution dismissal and barring even if there is no criminal prosecution.

3.2 Illegal Material. It is illegal to possess or distribute indecent images of a person under 18 and viewing such images on-line may constitute possession even if not saved. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven will invariably lead to the individual being barred from work with children and young people.

3.3 Material which incites hate, harm or harassment. There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress of anxiety.

3.4 Professional inappropriate material. Actions outside the workplace that could be considered so serious as to fundamentally breach the trust and confidence in the employee may constitute Gross Misconduct. These actions may not always be illegal, for

example, using work equipment to access inappropriate or indecent material, including 'adult pornography', will given the academy or service rightful cause for concern particularly if as a result learners or young people might be exposed to inappropriate or indecent material. Such behaviour would be considered inappropriate and could result in disciplinary action.

3.5 Some examples of inappropriate material and actions are:

3.5(a) Posting offensive or insulting comments about colleagues on social networking sites.

3.5(b) Accessing adult pornography on work-based computers during break.

3.5(c) Making derogatory comments about learners or colleagues on social networking sites.

3.5(d) Posting unprofessional comments about ones professional or workplace on social networking sites.

3.5(e) Making inappropriate statements or asking inappropriate questions about students on social networking sites.

3.5(f) Contacting learners by email or social networking without senior leadership team approval.

3.5(g) Trading in fetish equipment or adult pornography.

3.6 For further guidance on what is considered 'Inappropriate Material' please refer to the LSCB website www.leedslscb.org.uk/Children-Young-People/Online-safety

4. Creating images of learners through photography and video

4.1 Many work-based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written permission should be gained from legal guardians as well as senior management prior to creating any images of learners.

4.2 Using images of learners for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the academy or service provision have access.

4.3 Photograph or video images must be created using equipment provided by the workplace. It is not acceptable to record images of learners on personal equipment such as personal cameras, mobile phones or video cameras without prior consent. Images of learners must not be created or stored for personal use.

4.4 Members of staff creating or storing images of learners using personal equipment without prior consent may be subject to disciplinary action.

4.5 Members of staff must:

4.5(a) Be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded.

4.5(b) Ensure that senior management is aware that photography/image equipment is being used and for what purpose.

4.5(c)v Ensue that all images are available for scrutiny in order to screen for acceptability.

4.5(d) Be able to justify images of learners in their possession.

4.5(e) Avoid making images in one to one situations.

4.6 Members of staff must not take, display or distribute images of learners unless they have consent to do so. Failure to follow any part of this code of practice could result in disciplinary action being taken.

4.7 For further guidance on creating, displaying and storing images of learners please refer to the LSCB website, Education Leeds Safer Working Practice guidance and DCSF guidance document Cyberbullying – Supporting School Staff.

5. Propriety and behaviour

5.1 All members of staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of learners and young people. They should adopt high standards of personal conduct in order to maintain the confidence and respect of their peers, learners and the public in general.

5.2 Members of staff should not behave in a manner which would lead any reasonable person to question their suitability to work with children or act as a role model. This includes behaviour in virtual online communities as well as day to day social situations. Members of staff also should not make (or encourage others to make) unprofessional persona comments through online media which scapegoat demean or humiliate, or might be interpreted as such.

5.3 An individual's behaviour, either in or out of the workplace, should not compromise his or her position within the work setting or bring the academy or organisation into disrepute.

5.4 If an allegation is received that a member of staff is responsible for comments made (online or otherwise) which could be deemed harmful, threatening, defamatory or abusive to the academy or organisation, this will be investigated using the appropriate procedure. Any actions which bring the organisation or profession into disrepute will be considered under the appropriate policy and appropriate action taken in line with that procedure.

5.5 For further guidance on Property and Behaviour please refer to Education Leeds Safer Working Practice guidance document April 2008.

6. Cyberbullying

6.1 All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Bullying and Harassment Policy and could result in disciplinary action.

6.2 However, this doesn't just extend to behaviour within the workplace. In some instances bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility for the employer and therefore result in disciplinary action being taken against the responsible individual.

6.3 Certain activities relating the cyberbullying could be considered criminal offences under a range of different laws. Cyberbullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

6.4 If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the organisation will investigate this matter. Any allegation of Bullying or Harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Bullying and Harassment policy and could lead to disciplinary action.

6.5 Staff are required to take steps to protect themselves and their personal information by:

6.5(a) Keeping all passwords secret and protect access to their online accounts.

6.5(b) Not befriending learners and young people on social networking services and sites.

6.5(c) Keeping personal phone numbers private.

6.5(d) Not using personal phones to contact parents and learners, children and young people.

6.5(e) Keeping personal phones secure, i.e. through use of a pin code, when within work.

6.5(f) Not posting information about themselves that they wouldn't want employers colleagues, learners, children, young people or parents to see.

6.5(g) Not retaliating to any incident.

6.5(h) Keeping evidence of any incident.

6.5(i) Promptly reporting any incident using existing routes for reporting concerns.

6.6 Any incident of cyberbullying will be investigated under the appropriate policy and could result in disciplinary action.

6.7 Further information and advice regarding cyber bullying can be found in the DCSF guidance document Cyberbullying – Supporting School Staff.

7. Rules for staff

7.1 Members of staff should adhere to the following rules:

7.1(a) access the system with own user name and password, which will not be divulged to anyone;

7.1(b) not to access another person's files;

7.1(c) not to logon with another person's username nor allow others, staff or learners, to use their own logon;
7.1(d) to logoff correctly and leave the equipments set up for the next person;

7.1(e) never to leave the computer unattended unless it has been logged off first or the desktop has been locked;

7.1(f) computers used for Temple Learning Academy business only during the normal daily teaching hours;

7.1(g) not attempt to access personal email during any learner contact time;

7.1(h) not to use my Temple Learning Academy email account for personal business nor use personal email for Temple Learning Academy business;

7.1(i) to abide by the Data Protection Act and only store learners' data if absolutely necessary;

7.1(j) not to store learners' data on removable drives including laptops unless it is encrypted;

7.1(k) to only email learner data to approved persons;

7.1(l) messages I send will be polite and responsible;

7.1(m) not to send anonymous messages or forward chain letters and not send messages which appear to come from someone else;

7,1(n) to report any unpleasant material or messages received;

7.1(o) not to compromise the security of ICT systems, whether owned by the school, or by other organisations or individuals (including attempting to bypass Internet security filters);

7.1(p) to not use my own software on the network;

7.1(q) to understand that copyright and intellectual property rights must be respected;

7.1(r) to understand that the academy may check my computer files, monitor the Internet sites I visit and the contents of my email messages;

7.1(s) to be economical with printing and preview and spell check my work before printing

7.1(t) not to copy or download music or video files to the academy network if it is for personal use;

7.1(u) to aim to keep files storage to a minimum and delete files not used regularly;

7.1(v) to limit personal internet access to outside contact/contracted time;

7.1(w) to not deliberately visit any internet sites that would be considered irresponsible in a place of work or education.

7.1(x) not to download any personal software onto academy computers whether in the academy or offsite, this includes software that you have a personal licence for or freeware (no licence required). If additional software is required by a member of staff they must request RM to install it and have copies of the complete licence agreement for the product. If the product is freeware then documentation must be produced showing that it can legally be installed onto a networked computer. Temple Learning Academy reserve the right to refuse software being installed onto the system or single computer if it is deemed inappropriate or if the licence documentation is inconclusive about being installed onto a networked computer.

Agreement
I have read and understood the Acceptable Use Policy above and agree to abide by its rules when using the ICT resources within the academy or when on academy business.

Staff member

Name: .....

Signature: .....

Date: .....

Staff who break these rules risk disciplinary action

SECTION 2 – LEARNERS

1. Temple Learning Academy's ICT acceptable use policy (AUP)

1.1 Temple Learning Academy's computing facilities are provided to enable learners to further their education and staff to enhance their professional activities including teaching, research, administration and management.

1.2 Learners will not be able to access the Internet until this form has been signed and returned. Permission to use the facilities is conditional upon their user signing an agreement to abide by the "Acceptable Use Policy". Any breaches of this policy will be treated as a disciplinary matter and dealt with appropriately. The use of a computer system without permission or for a purpose not agreed by the academy could constitute a criminal offence under the Computer Misuse Act 1990. The academy may exercise its right, including by electronic means, to monitor the use of the academy's computer systems, including the monitor of websites visited, the interception of emails and the deletion of inappropriate materials in circumstances where it believes unauthorized use of the academy's computer system is, or may be taking place, or the system is or may be being used for criminal purpose or for storing text imagery which is unauthorised or unlawful. Where misuse of the system is suspected the Network Manager will immediately remove the user's access rights pending an investigation. The academy has installed computers with Internet access for the purpose of its business.

2 Rules for learners

2.1 Learners will sign a declaration form agreeing to the following rules:

2.1(a) I will access the system with my own user name and password, which will not be divulged to anyone;

2.1(b) I will not to access another person's files;

2.1(c) I will not to logon with another person's username nor allow others, staff or learners, to use my own logon;

2.1(d) I will logoff correctly and leave the equipments set up for the next person;

2.1(e) I will never to leave the computer unattended unless it has been logged off first or the desktop has been locked;

2.1(f) I will use my computer for Temple Learning Academy business only during the normal daily learning hours;

2.1(g) I will only send messages that are polite and responsible;

2.1(h) I will not send anonymous messages or forward chain letters and not send messages which appear to come from someone else;

2.1(i) I will report any unpleasant material or messages received;

2.1(j) I will not to compromise the security of ICT systems, whether owned by the academy, or by other organisations or individuals (including attempting to bypass Internet security filters);

2.1(k) I will not use my own software on the network;

2.1(l) I understand that copyright and intellectual property rights must be respected;

2.1(m) I understand that the academy may check my computer files, monitor the Internet sites I visit and the contents of my email messages;

2.1(n) I will be economical with printing and preview and spell check my work before printing

2.1(o) I will not copy or download music or video files to the academy network if it is for personal use;

2.1(p) I will aim to keep files storage to a minimum and delete files not used regularly;

2.1(q) I will limit personal internet access to outside contact/contracted time;

2.1(r) I will not deliberately visit any internet sites that would be considered responsible in a place of education.

2.1(s) I will not copy or download music or video files to the academy network if it is for personal use and without permission.

2.1(t) I will not listen to online music/videos, without my teacher's permission.

2.1(u) I will not take photographs or video of anyone without their permission

2.1(v) I will only access websites my teacher has allowed, and will not use the academy ICT systems for on-line gaming, on-line gambling, internet shopping file sharing, videos broadcasting (e.g. YouTube), or accessing social networking sites (e.g..BeBo).

2.1(w) I will not create websites, social networking groups or any kind of web gathering for any member of staff.

2.1(x) I promise that I shall not intentionally damage the hardware loaned to me and any damage occurred to the equipment shall be repaired/replaced at a cost to me.

2.1(y) I shall only use the 3G dongle provided to access the internet and use my own personal Leeds Learning Network username and password.

2.1(z) I promise to return the equipment in the same condition as when it was loaned to me.

Learners who break these rules risk disciplinary action.

Agreement
I have read and understood the Acceptable Use Policy above and agree to abide by its rules when using the ICT resources within the academy or when on school business.

Learner
Name: .....
Signature: .....
Date: .....

Parent/Guardian
Name: .....

Signature: .....
Date: .....

SECTION 3 - ICT NETWORK USAGE POLICY

1. General purpose of the policy

1.1 The purpose of this policy is to inform users of the Temple Learning Academy ICT network how it should be used and where user responsibilities are. It will give guidance as to what is expected when they use the network or any systems belonging to Temple Learning Academy and Leeds Education Authority.

1.2. This policy will cover:

1.2(a) General use

1.2(b) Security

1.2(c) Internet

1.2(d) Email

1.2(e) File storage and management

1.2(f) Responsibilities

1.2(g) Personal use

1.2(h) None Temple Learning Academy Equipment

1.2(i) Help Desk

2. General use

2.1 The purpose of this ICT network is to provide support for staff in carrying out the business of Temple Learning Academy. This will be the overriding principle used when considering any use made that may be unclear from reading any part of this policy:

2.1(a) ICT equipment should only be used for TMHS business.

2.1(b) The Data Protection Act of 1998 should be used when dealing with confidentiality.

3. Security

3.1 Security covers three areas. That of the physical security of equipment, data and system integrity.

3.2 It is the responsibility of each member of staff to look after the physical security of all academy equipment. The main way of securing equipment is by regular monitoring and keeping equipment locked when not in use or being monitored by a member of staff:

3.2(a) Data – all data should be kept secure and backed up. It is the responsibility of the ICT support staff to maintain a back up of all data on the network. However, it is recommended that all staff have some form of backup system for work kept on USB, pens, CD's, Portable Hard Disks and locally on laptops (including TMHS laptops). Please note that the data on laptops, USB pens, DVD/CD and Portable hard disks are not secure (see the 'Computer Information and Security Policy').

3.2(b) Systems Integrity - access to the computer system will be made available on a needs only basis.

3.2(b)i Software – **No** software should be installed by any member of staff without permission of the Network Manager. It is all members of staff's

responsibility to make sure that the learners do not install software on the computer system.

3.2(b)ii Attaching external devices – **No** hardware should be connected to the computer system without approval of the Network Manager. This does not apply to file transfer systems.

3.2(b)iii File transfer systems i.e. USB memory pens. It is the responsibility of each member of staff that files transferred to or from the network are first of all virus checked and that they have permission to transfer the file. Acceptable files are any that relate to Temple Learning Academy business, unacceptable files are those that are unacceptable type, nature or not for Temple Learning Academy business.

4. Confidentiality

4.1 It is the responsibility of all staff to keep all confidential data secure and that they conform to the Data Protection Act.

4.2 Confidential data should only be divulged to those who have a need. Any confidential files must only be transferred offsite if there is a specific reason for that file or data to be transferred, it is then the responsibility of the transferee to make sure confidentiality is maintained. For more information see the 'Computer Information and Security Policy'

5. Passwords

5.1 The following points need to be noted when creating passwords:

5.1(a) are at least 8 characters in length;

5.1(b) contain characters from three of the four categories: uppercase; lowercase; 0 through to 9;or special characters (*&^%$£"! etc);

5.1(c) do not repeat sequences i.e. Banana#1 then Banana#2;

5.1(d) changed on a regular basis (minimum each half term);

5.1(e) are not stored on paper, diaries etc;

5.1(f) are not divulged to any other person.

6. Computer access

6.1 If you logon to a computer then leave the room you must log off so that other staff can use the computer. If you can guarantee you will be away for a few minutes then you must lock the computer using Ctrl, Alt, Del, and select "Lock this computer". Never leave the computer unlocked.

6.2 When you have finished with SIMS, shut the program down.

6.3 Never allow learners to use a computer that a member of staff is logged onto.

7. Internet

7.1 The Internet is an excellent source of information, unfortunately that information may be incorrect or of an inappropriate nature. As such the use of the internet within the academy is of a sensitive nature; BECTA is an excellent source for detailed information. The academy and Leeds City Council have extensive filtering and monitoring systems in place, however, due to the fluid nature of the Internet, this will never replace personal

responsibility and due diligence. Unfortunately, the consequence of misuse of the Internet has lead to certain resources and systems being made inaccessible i.e. MSN, Skype.

7.2 Use the following points as guidelines when using the Internet for personal, business and classroom use:

7.2(a) Do not use computer or the internet as a reward as part of you classroom management.

7.2(b) Do not use or allow the use of any form of Chat or Social networking, use the academy graduated response policy with learners who break the rules.

7.2(c) Do not use or allow the use of computers or Internet for playing games, unless educational.

7.2(d) Check websites during lesson planning (websites are removed by the owner daily).

7.2(e) Inaccessible websites have been filtered for a reason, please respect that when lesson planning. ICT support staff always investigates a site before filtering it. Filtering a site is quick; un-filtering a site takes time.

7.2(f) Requests for un-filtering of a website should be made by email to IT Support (and must include the exact site URL and justification. Removal of filtering could take up to 24 hours as the site is checked fist. If the site is filtered by LLN then it may take up to 5 days. Email confirmation will be sent as soon as a decision is made.

7.2(g) If the website has been allowed or disallowed by previous staff requests then they will be contacted before any decision is made to re allow or disallow a site.

7.2(h) Forensic monitoring may be installed as a government requirement, this will allow the detailed monitoring of the internet traffic and content by the Principal or his delegate.

8. Email

8.1 Guidelines for the use of the TLA email system:

8.1(a) only use the TLA email for business;

8.1(b) checking personal emails is not allowed in academy at this time;

8.1(c) all emails may be monitored;

8.1(d) the content of any TLA email is the property of TLA;

5.1(e) be very careful transferring confidential information by email, use the security guidelines earlier in this document;

5.1(f) do not email pictures of learners;

5.1(g) keep attachments to a minimum there is limit of 5MB;

5.1(h) if possible store the attached file in the staff shared area and email a link.

9. File storage and management

9.1 After the running of programs, storage of files is the main use of a computer network. It is also one of the main problems when managing a network. This is caused by staff and learners storing excessive amounts of files and inappropriate files i.e. personal images, personal music and video files.

9.2 All staff must get into the habit of archiving to CD/DVD of all old files specifically image and media files as they take up a significant amount of storage capacity.

9.3 Responsibility and accountability for file storage areas:

9.3(a) My Documents – these file areas are accessible only by individual users and Network Manager. Access is controlled by password to staff who are responsible and accountable for the content of these areas. All Staff Home Directories are limited to 400MB.

9.3(b) Staff shared areas - this is the storage area for departmental and general staff files. All staff must make sure that they store files only with their departmental areas. The responsibility and accountability for these files storage areas is with the curriculum co-ordinators.

9.3(d) Learner shared areas - the file location is for staff to place files and documents for 'read only' access by learners. To use the file learners should copy the files to their own My Documents. To make it easy for learners to find this area it must be kept organised and that will be the responsibility of curriculum departments.

9.3(e) Other file locations – a specific member of staff will be nominated to be responsible a accountable for these areas.

9.3(f) Media files – these are the main cause of over capacity problems with file storage, and as such some basic points should be followed:

9.3(f)i Images for learners should be resized to 640x480 wherever possible, especially the files that will be downloaded to MY Documents by multiple students.

9.3(f)ii Learners should be encouraged to delete them when the project is finished

9.3(f)iii Video files should be kept to a size of 30MB or less using compression methods and keeping the duration short <3min.

9.3(f)iv Video files should not be copied to the learners shared and then to their My Documents unless absolutely necessary. They should then be deleted as soon as possible.

9.3(f)v Music files must not be stored in any staff or learners personal area unless it is specifically for curriculum use. They must be removed as soon as they are no longer required.

9.3(f)vi The usage of these types of files will be closely monitored.

10. Network Folders

10.1	Staff	400MB
10.2	Learners	100MB
10.3	Staff (shared)	250GB (shared)
10.4	Learners (shared)	250GB (shared)

11. Responsibility

11.1 It is the responsibility of all network users to look after the ICT equipment that they use and to report any problems as soon as possible. All users are responsible for any data they access and use. Each user must always take into account data and security or confidentiality. The following points are in addition to normal working responsibilities:

11.1(a) members of staff are responsible for all equipment they use and is used by learners under their supervision;

11.1(b) members of staff must report any misuse or damage as soon as possible;

11.1(c) members of staff are responsible for taking any action against learners misusing the equipment or using the computers inappropriately;

11.1(d) ICT technicians are the only persons who should carry out any repairs to equipment;

11.1(e) ICT technicians are responsible for backing up and files that are stored on the servers;

11.1(f) users are responsible for any files not stored on a server or stored locally on laptops;

11.1(g) ICT technicians will carry out routine maintenance;

11.1(h) Curriculum co-ordinators are responsible for maintaining the files under their subject area and for making sure that they do not exceed the maximum capacity;

11.1(i) users are responsible for removing unwanted images as soon as they are no longer necessary ICT technicians will back these up to CD on request.

12. Personal use

12.1 The TLA computer network is for business use; it is provided to assist members of staff in the delivery of the curriculum and to provide a means of enhancing teaching and learning. In an academy environment it is difficult to monitor the specific uses of computers and to decide if the use is business or personal. However, it must be made clear that members of staff are responsible and accountable for how they use the computer network, what files are stored within their personal storage areas and keeping passwords secure.

12.2 Sharing your password does not allow you to abdicate responsibility. Use the following as a guideline:

12.2(a) No personal use during contact time.

12.2(b) Restrict personal use to 1hour a day and outside normal working hours.

12.2(c) Do not use the computer in the presence of learners.

12.2(d) Do not store personal files on the academy network or laptop.

12.2(e) Make sure that you are away from a computer for at least 30 minutes of the lunch break.

12.2(f) Remember that the Principal or a person nominated by him has the right of access to any file or location on the network or on equipment owned by the organisation.

13. Non-Temple Learning Academy equipment

13.1 Personal laptops or computers must NOT be connected to the network without prior agreement of the Principal or Network Manager. This will only be given when proof of an installed and up to date security system is shown.

13.2 All personal equipment brought into the academy is done so at the owners risk and is not covered by TLA and LLN insurance.

13.3 No mains electrical equipment can be used unless it has been approved and PAT tested first.

14. IT Support

14.1 IT Support are here to tackle any of the faults you find with the ICT equipment, or, if staff have an ICT related request i.e. putting new software onto the system.

14.2 Below is a list of tasks that IT Support should be notified of, so they can be resolved:

14.2(a) Faulty ICT equipment;

14.2(b) requesting passwords and usernames of learners;

14.2(c) removing Internet or full computer access from learners due to a recorded incident;

14.2(d) putting new software onto the system (a full licence and proof of purchase must be provided);

14.2(e) software or hardware query;

14.2(f) request to block or unblock websites (see Internet section in this document);

14.2(g) requesting a SIMS username and password.

14.3 IT can be contacted by members of staff via the following methods depending upon the problem to be resolved: Email; Telephone: 08450 264682 or, Log a fault at the academy reception if the problem requires an On-call and immediate resolution if it halting the teaching of a lesson or log a problem directly through the RM Portal.

14.4 Important Information_- only critical problems are the exception for this. For reference, critical tasks include, but are not limited to:

14.4(a) more than 30% of the rooms computers not in a functional state;

11.4(b) problems that are essential and need to be fixed within the next hour. We have the right to confirm, if the problem is essential and will advise you to use the RM support online service;

11.4(c) unforeseen requirements for visitors. (booking must still have been made).

14.5 Non-critical tasks:

11.5(a) broken keyboard/mouse/monitor;

11.5(b) workstation and or printer not working;

11.5(c) software not working as expected;

11.5(d) student cannot log on.

14.6 Bookings. If you require a room setting up with ICT equipment for a session or guest speaker, this can be requested via e-mail to the Leeds support. This must be done a week in advance of the event.

SECTION 4 – COMPUTER INFORMATION AND SECURITY POLICY

1. Purpose of the policy

1.1 This policy covers the security and confidentiality of data stored on the computer network and data transferred electronically. It gives guidelines for, and defines the responsibilities of users and covers the following:

1.1(a) use of passwords;

1.1(b) information stored on the network computer in:

1.1(b)i staff shared locations

1.1(b)ii personal - My Documents

1.1(b)iii SIMS

1.1(b)iv TLA information stored on non-TLA computers;

1.1(c) information stored in laptops;

1.1(d) information stored on USB pens, CDS, DVDS etc;

1.1(e) information transferred electronically via email or other media;

1.1(f) information downloaded onto personal Computers at home or away from the business site;

1.1(g) back-up procedures:

12.2(g)i network;

12.2(g)ii laptop.

1.2 Security is the responsibility of the person holding or accessing information. Reference will be made to the Data Protection Act which is explained in brief on the last page of this policy.

2. Passwords

2.1 All passwords should be unique and follow the following basic format.

2.2 All passwords are at least 8 characters in length and contain characters from three of the four categories:

2.2(a) uppercase

2.2(b) lowercase

2.2(c) 0 through 9, or

2.2(d) special characters (*&^%$£”! etc.)

2.3 All passwords should be changed frequently at least every half term. If you suspect that someone has seen your password it must be changed immediately. If you catch anyone using your password this must be reported immediately to a member of senior management team. Passwords should not be divulged to any person not employed by TLA|. This includes computers at home that contain TLA confidential information or have access to the academy email without using your email password.

2.4 Email passwords should be different from network passwords.

2.5 TLA passwords must be different from personal ones.

3. Transfer of information

3.1 Confidential information must only be transferred to a secure location and only be kept as long as it is necessary. Always delete confidential information when it is no longer required or is inaccurate (please remember to empty to recycle bin). When transferred to a portable device i.e. laptop or USB pen then that device must be kept secure and any loss reported immediately.

3.2 Information transferred to another person or organisation should be carried out only when absolutely necessary and only then to an approved person or organisation and must only be done using a secure method, see later.

4. Laptops

Laptops are not secure; even those with a strong password. If a laptop is stolen or physically accessed by an unauthorised person, then any file on the laptop can be accessed within minutes without knowledge or your password or username.

5. Portable media: USB pens, CDs, DVDs etc.

5.1 Care should be taken when transferring data using these methods as they are easily lost.

5.2 CDs and DVDs should not be used if possible as they are frequently left lying around when finished with and should be destroyed as soon as possible. Members of staff should make sure you explain this to outside organisations and individuals.

6. Email

6.1 It is the academy's policy that we do not email any confidential information to email addresses other than the academy email addresses as we cannot guarantee its security.

6.2 The academy's email is web-based and is stored within Leeds Learning Network firewall. If information has to be emailed to an external individual or organisation then their email security policy should be checked first and that it will conform to the Data Protection Act. If possible the information should be encrypted before being sent.

7. Home computers

7.1 To ensure total security the home computer must use a home logon password protected system so access to any confidential information is restricted to academy staff only. This only applies when information is transferred to the home computer via USB pen, email etc.

7.2 No academy password should be saved on the computer and must be entered every time the information or email is accessed. If work is carried out only on USB pens then that device should be kept secure and not loaned to a member of staff's family unless confidential information is erased.

8. Back-up

8.1 Data and information security also covers the protection against loss due to device failure or human error. Always back up any data that is saved on a laptop or USB pen. The information on this back-up should be treated as confidential and kept secure using locked filing cabinets etc. When a back-up CD or DVD is obsolete it must be destroyed.

8.2 When working on a network computer or a laptop that is connected to the network then any file saved to My Documents or any shared area will be backed up automatically every day.

8.3 USB pens are fragile and can easily be damaged by being removed from the computer in an unsafe manner or heat etc. They should be backed-up to a reliable and safe area as soon as possible i.e. networked My Documents.

9. Secure folders and encryption

9.1 Network files are secure as the password, servers are usually physically secure and direct access is required to overcome a good logon and password. Laptops USB pens, CDs etc are not physically secure and are therefore vulnerable to information theft.

9.2 Using secure folders that are encrypted is the normal solution; Windows XP has the facility to encrypt files that ensures they can only be opened by using the logon or password of the person who encrypted them even if the computer is physically stolen. However, if the computer fails and the files recovered, it may not possible to encrypt them. Any backups are unencrypted so are at risk.

9.3 An alternative method of securing files and folders is to encrypt them using third party software. These programs usually use a second password which enables the secure files be opened on any computer that has the third party software and the password. A free and recommended software that does this is TrueCrypt. This enables the encrypted information to be stored in a removable media securely.

9.4 When data is to be transferred then encryption should be used that does not require any special software to decrypt and open. An easy solution is to use WinZip and password protect the Zip file. When sent to another person by email they can pen the file if they have the password which should be sent separately preferably using a different method.

9.5 If you have any questions regarding this policy please contact your ICT support personnel.

SECTION 5 - NEW USER NETWORK AND SIMS NOTIFICATION

1. Network and SIMS access

1.1 To generate a network and SIMS logon request, the following information should be emailed to RM Support by the member of staff requesting a username and password. An email will be sent back to you with this information. (Please note: it is the responsibility of all staff to keep their network and SIMS password secure. At no time must a computer be left logged on nor should learners be allowed to use a computer where a member of staff is logged on. In particular, SIMS should never be left unattended, even when teaching in the same classroom and using the computer as a teaching aid.)

1.2 Please read the 'ICT Network Policy' and the 'Computer Information and Security Policy 'both of these are available on the shared area and the VLE.

1.3 Please change your network password at first logon using a minimum of 8 characters with at least one uppercase letter and a number or symbol.

2. Access to email log

To access your email log on the Internet, you can either go to 'Your' Email or Mysite.

3. Breaches of security

All breaches of security must be reported to the Network Manager or Data Manager if it is a SIMS issue, as soon as it occurs.

SECTION 6 – DATA PROTECTION ACT 1998

In brief the Data Protection Act 1998 states:

1. Data may only be used for the specific purposes for which it was collected.

2. Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (for example, the prevention or detection of crime). It is an offence for 'other parties' to obtain this personal data without authorization

3. Individuals have a right of access to the information held about them, subject to certain exceptions (for example, information held for the prevention of crime).

4. Personal information may be kept for no longer than is necessary.

5. Personal information may not be transmitted outside the establishment unless the individual to whom it is about has consented or adequate protection is in place, for example, by the use of a prescribed form of contact to govern the transmission of the data.

6. Subject to some exceptions for organizations that only do very simple processing and for domestic use, all entitles that process personal information, must register with the Information Commissioner.

7. Entitles holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organizational (such as staff training).