Beckfoot
Trust

Beckfoot
Upper Heaton

Keeping Children Safe in Education

eSafeguarding Policy

Title		Campus eSafeguarding policy	
Version		0.2	
Date		1/2/2017	
Author		Simon Wade	
Approved by Headteacher			
Approved by Board of Directors			
Next review date		September 2017	
Modification history			
Version	Date	Description	Revision author
0.1	*April 2015*	*New Campus version created from previous Beckfoot/Hazelbeck eSafeguarding Policies*	*Simon Wade*
0.2		*Approved by Board of Directors*	

Beckfoot Upper Heaton School is a new, mixed comprehensive school with 450 students, including approximately 40 within the Sixth Form. It was formed in September 2015 as part of the Beckfoot Trust. Our core purpose is for all learners to enjoy school, become independent learners and to expect success. Our job is to equip every learner with the skills and qualities needed to be successful in an ever changing world. Indeed, our school motto: 'ENJOY – LEARN – SUCCEED' very much reflects our ethos.

We are very ambitious. We want to become one of the finest examples of comprehensive education in the country. We passionately believe that every young person has talent and it is the job of a good school to ensure that they fulfil it. We are dedicated to breaking the link between family income and educational achievement, ensuring that children from all backgrounds can fulfil their potential and make the most of their talents.

Contents

Policy introduction

The campus eSafeguarding policy has been written to ensure safety measures are in place to protect both students and staff working with ICT equipment and related technologies in Beckfoot Upper Heaton. The policy is to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and students' standards and practice. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to eSafeguarding by knowing the content of the policy and the procedures adopted and developed by the school.

Scope of policy

- This policy applies to the whole campus community including the Senior Leadership Team of Beckfoot Upper Heaton, the Board of Directors and all staff employed directly or indirectly by the school and all students.
- The Board of Directors and the leadership team of Beckfoot Upper Heaton will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or students when they are off the school site. This is pertinent to incidents of cyberbullying, or other eSafeguarding related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of school.

Review and Ownership

- The campus eSafeguarding policy has been written by the eSafeguarding Coordinators of both schools, and is current and appropriate for its intended audience and purpose.
- The campus eSafeguarding policy has been agreed by the senior leadership team and approved by the Board of Directors
- The campus eSafeguarding policy will be reviewed annually or when any significant changes occur with regards to the technologies in use within the school.
- The School has an appointed member of the Board of Directors to take lead responsibility for eSafeguarding.
- Amendments to the campus eSafeguarding policy will be discussed in detail with all members of teaching staff.

The Responsibility of the Senior Leadership Team

We believe that eSafeguarding is the responsibility of the whole campus community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The executive head teacher is ultimately responsible for Safeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator.

- The head teachers and leadership teams are responsible for ensuring that the eSafeguarding Coordinators and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The leadership teams will receive monitoring reports from the eSafeguarding Coordinator.
- The head teachers and leadership teams should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.
- The head teachers and leadership teams should receive update reports from the incident manager.

The Responsibility of the eSafeguarding Co-ordinator

- To promote an awareness and commitment to eSafeguarding throughout the school.
- To be the first point of contact in school on all eSafeguarding matters.
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures.
- To have regular contact with other eSafeguarding committees, e.g. the local authority, Local Safeguarding Children Board.
- To communicate regularly with school technical staff.
- To communicate regularly with the designated eSafeguarding member of the Board of Directors.
- To communicate regularly with the senior leadership team.
- To create and maintain eSafeguarding policies and procedures.
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- To ensure that eSafeguarding education is embedded across the curriculum.
- To ensure that eSafeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on eSafeguarding issues to the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- To understand the issues surrounding the sharing of personal or sensitive information.

Responsibility of Teachers and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with students should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social networking etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide students carefully when engaged in learning activities involving technology.
- To ensure that students are fully aware of research skills and methods.
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times.

Responsibility of Technical Staff

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.

- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Responsibility of Students

- Students will understand and adhere to the school Student Acceptable Use Policy.
- Students with a lower level of cognition will require a parent/guardian to sign on their behalf the school student AUP.
- To help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates.
- Students will be expected to understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school rules relating to bullying and cyberbullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exists within school.
- To discuss eSafeguarding issues with family and friends in an open and honest way.

Responsibility of Parents and Carers

- To help and support the school in promoting eSafeguarding.
- To read, understand and promote the school student Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology.
- To consult with the school if they have any concerns about their children's use of technology.
- To annually agree to and sign the home-school agreement.
- To annually agree and sign the photography permission form stating where photographs are to be published.

Responsibility of the Board of Directors

- To read, understand, contribute to and help promote the campus eSafeguarding policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by students.
- To develop an overview of how the campus ICT infrastructure provides safe access to the internet.
- To develop an overview of how the campus encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the school campus to implement its eSafeguarding strategy.
- To develop an overview and understanding as the body corporate in relation to their responsibilities regarding the schools Data Protection commitments.

Responsibility of Child Protection Officer(s)

- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of other external groups

- The schools will liaise with local organisations to establish a common approach to eSafeguarding and the safe use of technologies.
- The schools will be sensitive and show empathy to internet-related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice where appropriate.
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within the schools.
- The schools will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds. (Parent helpers, trainee teachers, work experience students etc.).

Managing Digital Content

- Before photographs of students can be published, permission must be granted formally via the photography policy, which has to be signed by parents annually. All staff are aware of the process involved with publishing images over different mechanisms.
- Parents and carers may withdraw permission, in writing, at any time. A procedure exists for permission to be removed retrospectively.
- We will remind students of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Students and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the head teacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and students involved.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites (optional - unless appropriate security settings are enabled and set to maximum).
- When searching for images, video or sound clips, staff will be taught about copyright and acknowledging ownership.
- When searching for images, video or sound clips staff will ensure that student's usage is monitored for copyright purposes.

Storage of images

- Any images, videos or sound clips of students must be stored on the school network and never transferred to personally-owned equipment. The schools will store images of students that have left the school for a number of 5 years following their departure for use in school activities and promotional resources.
- Students and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of students.
- The network manager has the responsibility of deleting the images when they are no longer required, or when a student has left the school. This instruction will come from a member of the Leadership Team once a procedure and agreement has been decided.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our students' lives, not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the internet brings.

We will discuss, remind or raise relevant eSafeguarding messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.

- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Students will be taught about the impact of bullying and cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Child line or the CEOP report abuse button.

Staff training

- Our staff receive regular information and training on eSafeguarding issues in the form of annual updates, termly where applicable.
- As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas.

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- Members of staff will access the internet using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow students to access the internet through their username and password. They will abide by the school AUP at all times.
- All students have a unique username and password for access to ICT systems.

Passwords

- A secure and robust username and password convention exists for all system access. (Email, network access, school management information system).
- All information systems require staff to change their password at first log on. Where appropriate students will be assisted by members of staff in this particular task.
- Staff should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Staff should change their passwords whenever there is any indication of possible system or password compromise.
- Student's passwords will be managed by the appropriate member of support/teaching staff and changed when is deemed appropriate.

- All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Staff are expected to comply with the following password rules;

    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.

    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser

New technologies

We will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafeguarding point of view. We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by students which may cause an eSafeguarding risk.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- The school will audit ICT equipment usage to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Mobile phones

Beckfoot Upper Heaton:

- Students should follow school rules if they decide to bring their mobile phone or personally owned device into school.
- Students should not use their mobile phone or other personally owned device to contact a parent or carer during the school day. If the need to do so arises they should liaise with their Pastoral Manager.
- Students are allowed to use their mobile phone or personally-owned device in school only during break and lunch times and in specially designated areas of the school.

Staff use of mobile devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Certain identified staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile phones and personally-owned devices will be stored securely with personal belongings within school.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work provided equipment for this purpose.

Filtering internet access

- The school’s internet provision will include filtering appropriate to the age and maturity of students.
- The schools will always be proactive regarding the nature of content which can be viewed through the school’s internet provision.
- The schools will have a clearly defined procedure for reporting breaches of filtering. All staff and students will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The schools will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked. ▯ Students will be taught to assess content as their internet usage skills develop.
- Students will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Internet access authorisations

- Parents will be encouraged to read the school Acceptable Use Policy for student access and discuss it with their children.
- All students will have the appropriate awareness training and where possible, sign the student Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that students will be provided with supervised internet access appropriate to their age and ability.
- The schools will maintain a current record of all staff and students who have been granted access to the schools' internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- When considering internet access for vulnerable members of the school community (looked after children) the schools will make decisions based on local knowledge.
- All students will be closely supervised and monitored during their use of the internet. Students will be frequently reminded of internet safety issues and safe usage.

Email

- Staff should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Where possible access to personal email accounts should be restricted to non-contact time and should be kept to a minimum.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and productivity and will be restricted in line with the school eSafeguarding and Acceptable Use Policies.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Staff will only use official school-provided email accounts to communicate with students and parents and carers, as approved by the senior leadership team and the Senior Information Risk Officer.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.
- Irrespective of how staff access their school email (from home or within school), school policies still apply. Emails sent to external organisations should be written carefully and, where necessary, authorised before sending to protect the member of staff sending the email.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school'.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations, parents or students, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.
- When away for extended periods, 'out-of-office' notification should be activated so that colleagues are aware that you are not currently available.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies need to be controlled and never communicated through the use of a personal account.

- Staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source but should consult the network manager first.
- Communication between staff and students or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within school should report any inappropriate or offensive emails through the incident reporting mechanism within school.
- Students must immediately tell a designated member of staff if they receive any inappropriate or offensive email.
- Students must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Students will be allocated an individual email account for their own use in school or class.
- Students may only use school-provided email accounts for school purposes.
- Whole class or group email addresses will be used in school for communication outside of the school.
- Students may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Students and staff will be reminded when using email about the need to send polite and responsible messages.
- Students and staff will be reminded about the dangers of revealing personal information within email conversations.
- Students must not reveal personal details of themselves or others in email communications.
- Students should get prior permission from an adult if they arrange to meet with anyone through an email conversation.

Using blogs, wikis, podcasts and other mechanisms to publish content online

- Blogging, podcasting and other publishing of online content by students will take place within the school learning platform or school website, www.beckfootupperheaton.org
- Students will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website/blog and postings should be approved by the head teacher before publishing.
- Staff will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

Use of Social Media

- Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.
- Staff and students are asked to report any incidents of cyberbullying to the school.
- Staff will raise any concerns about student use of social media sites with parents/carers this includes the use of any sites that are not age appropriate.
- All staff will receive training on the risks associated with the use of social media either through staff meetings or via the induction process for new starters. Safe and professional behaviour is outlined in the Acceptable Use Policy.
- Staff must not use social media tools to communicate with current or former students under the age of 18.
- Staff will not use any social media tools to communicate with parents unless approved in writing by the head teacher.
- Procedures for dealing with cyberbullying incidents of staff or students involving social media are outlined in the school Anti-Bullying Policy.
- Parents/Carers will be reminded of their responsibilities in relation to the use of social media via the Home School Agreement and via the school website.
- Staff are advised to set and maintain profiles on such sites to maximum privacy and to give access to known friends only.

Data protection and information security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Alt-Del or equivalent) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the Senior Information Risk Officer and the applicable Information Asset Owner.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the Senior Information Risk Officer or Information Asset Owner.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/least privilege basis. All access should be granted through the Senior Information Risk Officer or Information Asset Owner.
- Staff and students will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- Fax machines will be situated within controlled areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, and encrypted removable media, remote access over encrypted tunnel.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Special requirements

We will seek to ensure that all users have access to ICT through the use of a range of specially adapted hardware.