KIRKBALK ACADEMY

Northern Education Trust

E-Safety Policy Suite

Academy Name: Kirk Balk Academy
Date adopted: 22nd September 2016
Review date: September 2017

Contents

1. Introduction and Overview

1.1 Rationale

The purpose of this policy is to:

- Set out the key principles expected at the academy of all members of the academy community with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of the academy
- Highlight issues affecting the use of ICT-based communication systems
- Assist academy staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other academy policies
- Ensure that all members of the academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students
- State the actions that may be taken to monitor the effectiveness of this policy suite
- Warn users about the consequences of inappropriate use of ICT-based technology and systems
- Establish a framework within which users of the academies ICT-based facilities can apply self-regulation to their use of academy ICT systems.

The main areas of risk for our academy community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites, including online radicalisation
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft including 'frape' (hacking Facebook profiles), other social media hacking and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online (internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

1.2 Scope

This policy applies to all members of the academy community (including staff, contractual third parties and agents of the academy, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are designated users of academy ICT systems, both in and out of the academy, including remote access. The use of ICT facilities by staff not authorised will be regarded as a disciplinary offence.

It covers all ICT facilities and communication systems provided by the academy for the purpose of conducting and supporting official business activity through the academies' network infrastructure and all stand alone and portable computer devices.

The Education and Inspections Act 2006 empowers Principals, to such an extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, radicalisation or other e-safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Academy Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of academy.

Staff and students have a responsibility to report any instances of witnessing or discovering blocked online searches or sharing of extremist or bullying messages or social profiles.

Any material/activity that the academy believes is illegal will be reported to the appropriate agencies including the Police, CEOP and IWF.

1.3 Roles and Responsibilities

Role	Key Responsibilities
Governors / E-safety governor Ms S Killshaw	• To ensure that the academy follows all current e-safety advice to keep the children and staff safe • To approve the e-safety policy and review the effectiveness of the policy. This will be carried out by the Governors/Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the academy in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include regular reviews with the E-Safety Coordinator/Officer (including e-safety incident logs, filtering/change control logs)
Executive Principal/ Vice Principal – Ms J M Nolan / Mr R Whitfield	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the academy uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. NGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To receive regular monitoring reports from the e-safety Coordinator/Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. Network Manager)

Role	Key Responsibilities
E-Safety Co-ordinator/ Designated Child Protection Lead Mr R Whitfield / Miss J Halliday	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the academy e-safety policies/documents • To promote an awareness and commitment to e-safeguarding throughout the academy community (e-safety section on the academy's website/leaflets) • To ensure that e-safety education is embedded across the curriculum • To Liaise with academy ICT technical staff • To communicate regularly with SLT and the designated e-safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date and any incidents are reported at Trust level • To facilitate training and advice for all staff • To liaise with the Trust, Local Authority and relevant agencies • To be regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: o sharing of personal data o access to illegal/inappropriate materials o inappropriate online contact with adults/strangers o potential or actual incidents of grooming o cyber-bullying and use of social media • To educate parents and raise awareness as instructed by the Trust, SLT and Governors
Heads of Academy/Computing Curriculum Leader Mr M Davies	• To oversee the delivery of the e-safety element of the computing curriculum • To liaise with the E-Safety Coordinator regularly
Network manager Mr R Smith	• To report any e-safety related issues that arise to the E-Safety Coordinator • To ensure that users may only access the academy's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the academy ICT systems • To ensure that access controls/encryption exist to protect personal and sensitive information held on academy-owned devices • To ensure that the academy's policy on web filtering is applied and updated on a regular basis • The internet service provider is informed of issues relating to the filtering they have applied • To keep up to date with the academy's e-safety policy suite and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure that the use of the network/Virtual Learning Environment (Learning Platform)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Coordinator/Vice Principal for investigation/action/sanction

Role	Key Responsibilities
	• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up to date documentation of the academy's e-security and technical procedures • To ensure that all data held on pupils on the Learning Platform is adequately protected
Vice Principal – Mr R Whitfield	• To ensure that all data held on pupils on the academy office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other academy activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended academy activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the academy's e-safety policy suite and guidance • To read, understand, sign and adhere to the academy ICT Acceptable Use Agreement (Appendix 1) • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement academy policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils are on a professional level and only through academy based systems, never through personal mechanisms, e.g. email, text, mobile phones, social media, etc.
Pupils	• Read, understand, sign and adhere to the ICT Acceptable Use Agreement • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To know and understand academy policy on the use of mobile phones, digital cameras and hand held devices • To know and understand academy policy on the taking/use of images and on cyberbullying • To understand the importance of adopting good e-safety practice when using digital technologies outside of the academy and realise that the academy's E-Safety Policy suite covers their actions outside of the academy, if related to their membership of the academy • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both inside the academy and at home • To help the academy in the creation/review of e-safety policies

Role	Key Responsibilities
Parents/carers	• To support the academy in promoting e-safety and endorse the ICT Acceptable Use Agreement which includes the pupils' use of the internet and the academy's use of photographic and video images • To read, understand and promote the academy ICT Acceptable Use Agreement with their children • To access the academy website/Learning Platform/online student/pupil records in accordance with the relevant academy ICT Acceptable Use Agreement • To consult with the academy if they have any concerns about their children's use of technology • To attend e-safety sessions delivered by the academy (where appropriate)
External groups	• Any external individual/organisation will sign an ICT Acceptable Use Agreement prior to using any equipment or the internet within the academy

1.4 Communication

How the policy will be communicated to staff/pupils/community in the following ways:

- Posted on the academy website/NET Portal/Learning Platform/staffroom/classrooms
- Policies to be part of the academy induction pack for new staff
- ICT Acceptable Use Agreements discussed with pupils at the start of each year
- ICT Acceptable Use Agreements to be issued to whole academy community, on entry to the academy
- ICT Acceptable Use Agreements to be held in pupil and personnel files

1.5 Handling complaints (Refer to Academy Complaints Policy)

- The academy will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an academy computer or mobile device. Neither the academy, the Trust or the Local Authority can accept liability for material accessed, or any consequences of internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - Interview/counselling by a member of the SLT or E-Safety Coordinator
    - Informing parents or carers
    - Removal of internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
    - Referral to Trust/Local Authority/Police
- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the SLT
- Complaints of cyberbullying are dealt with in accordance with our Anti Bullying Policy. Complaints related to child protection are dealt with in accordance with academy / Trust / LA child protection procedures

1.6 Review and Monitoring

The e-safety policy suite is referenced from within other academy policies: - ICT Acceptable Use Agreements, Child Protection Policy, Anti Bullying Policy, Safeguarding Policy, PREVENT policy, Information Assurance Policies, Data Protection Policy, Behaviour Policy, Critical Incident Management Plan and in the School Development Plan.

- The academy has an E-Safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the academy
- The e-safety policy template has been written by NET in collaboration with the academies. The template has been updated with the relevant local ICT arrangements by the academy's ICT Coordinator and is current and appropriate for its intended audience and purpose
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the academy e-safety policy suite will be discussed in detail with all members of teaching staff

1.7 Policy Compliance

If any user is found to have breached this policy, they may be subject to the academy's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Mr R Whitfield – Acting Vice Principal

- Users must familiarise themselves with the detail of this policy before using any of the academy ICT facilities on or offsite
- It is the user's responsibility to use all computer devices in an acceptable way. This includes not installing software that has not been approved, taking due care and attention when transporting and storing the equipment and not emailing CONFIDENTIAL information to a non-academy email address unless encrypted
- Users should be aware of the physical security dangers and risks associated with working with ICT equipment offsite
- It is the user's responsibility to ensure that access to all CONFIDENTIAL information is controlled – e.g. through password controls and encryption
- All CONFIDENTIAL data held on portable computer devices must be encrypted
- Whilst respecting the privacy of authorised users, the academy maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of removable media by authorised users to ensure adherence to this policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of items from removable media does not necessarily result in permanent deletion
- In addition to routine monitoring and audits, where a manager suspects that academy ICT equipment is being abused or misused by a user, they should inform Mr R Whitfield Should an investigation be authorised, designated staff may carry out an Internal Audit
- In addition, the academy will comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for information

1.8 Applying the Policy

All IT equipment (including portable computer devices) supplied to users is the property of the academy. It must be returned upon the request of the academy. Access for ICT Services staff of the academy shall be given to allow essential maintenance security work or removal, upon request.

All IT equipment will be supplied and installed by the academy IT staff. Hardware and software **must only** be provided by the academy.

2. Education and Curriculum

2.1 Pupil e-safety curriculum

This academy has a clear, progressive e-safety education programme as part of the Computing curriculum /Learning guide programme. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files - such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- To know how to report any abuse including cyberbullying; and how to seek 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 Childline or the CLICK CEOP button
- To plan internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas
- To remind students about their responsibilities through an end-user ICT Acceptable Use Agreement, which every student will sign/will be displayed throughout the academy
- To ensure staff will model safe and responsible behaviour in their own use of technology during lessons
- To ensure that, when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights
- To ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop ups; buying online; online gaming/gambling; SPAM email

2.2 Staff and governor training

This academy:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on e-safety issues and the academy's e-safety education program (annual updates/termly staff meetings etc.)
- Provides, as part of the induction process, all new staff [including those on university/academy placement and work experience] with information and guidance on the e-safety policy suite and the academy's ICT Acceptable Use Agreement

2.3 Parent awareness and training

This academy runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the ICT Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets; academy newsletters; on the academy web site
- Demonstrations, practical sessions held at the academy
- Suggestions for safe internet use at home
- Provision of information about national support sites for parents

3. Expected Conduct and Incident Management

3.1 Expected conduct

In this academy, all users:

- are responsible for using the academy ICT systems in accordance with the relevant ICT Acceptable Use Agreement, which they will be expected to sign before being given access to academy systems
- need to understand the importance of misuse or access to inappropriate materials and be aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies outside of the academy and realise that the academy's E-Safety Policy covers their actions outside of the academy, if related to their membership of the academy
- will be expected to know and understand academy policies on: (See ICT Acceptable Use Agreement)

    - Network Protocol
    - Passwords
    - Hardware & Software Downloads
    - Use of Data
    - Academy Email System
    - Use of images/Videos
    - Internet use
    - Mobile devices
    - Social networking
    - Remote Access

Staff:

- are responsible for reading the academy's e-safety policies and using the academy ICT systems accordingly, including the use of mobile phones, and hand held devices

Students/Pupils:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers:

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the ICT Acceptable Use Agreement at time of their child's entry to the academy
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

3.2 Incident Management (Refer to the Incident and Continuity Management Plan)

In this academy:

- There is strict monitoring and application of the e-safety policy suite and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely a need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the academy's escalation processes
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents take place and contribute to developments in policy and practice in e-safety within the academy. The records are reviewed/audited and reported to the academy's senior leaders, Governors and the Trust
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- If any apparent or actual internet misuse appears to involve illegal activity such as:
    - Child sexual abuse images
    - Adult material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Extremism or radicalisation of individuals
    - Other criminal conduct, activity or materials
- If information/data is compromised, lost or stolen it must be reported immediately to the Principal and NET Head Office who will deploy the Incident and Continuity Management Plan. Please see the Data Security breach Policy for further information

The academy should refer to the incident management flow chart in Appendix 4 which is an extract from the Incident and Continuity Management Plan to manage all ICT/data incidents.

3.3 Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that, where possible, the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use, e.g. put away in cupboard, locked in cabinet etc.

Users must ensure that access/authentication details and personal identification numbers are kept in a separate location to the portable computer device at all times. All removable media devices and paper

documentation must also not be stored with the portable computer device. Passwords and/or other access information should not be written down and stored near the portable device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Where personal and sensitive information is being printed on shared printers extreme care should be taken to ensure **all** documents are collected from the printer and that interruptions to printing due to paper jams, empty paper trays etc. do not lead to sensitive documents being discovered by unauthorised staff. Where personal and sensitive information is being printed, pin protection facilities, where available, should always be used. This will ensure documents are only printed when the appropriate person is at the printer to collect them and has an access code to do so.

Waste paper containing CONFIDENTIAL information must be shredded to required standards. If paper documents containing sensitive information are taken outside the office, the number of documents/cases should be limited in the same way as electronic records.

3.4 Access Controls

It is essential that access to all CONFIDENTIAL information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must be encrypted. If this is not possible, then all CONFIDENTIAL data held on the portable device must be encrypted. It is academy policy to encrypt/lock all laptops.

Remote users' access to academy systems (if connecting over public networks, such as the Internet) will need to be via VPN (and the 3rd party IT provider). No other access routes can be used.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to CONFIDENTIAL information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as the academy itself.

3.5 Emergency Recovery

The main contacts for emergency recovery of data for an individual pupil/staff member are listed below. For a full/part system failure refer to the critical incident continuity plan

Name	Position	Contact
Mr R Smith	Network Manager	rsmith@kirkbalkacademy.org
Mr A Scarfe	ICT Technician	ascarfe@kirkbalkacademy.org

All system critical equipment is covered by Microsoft DPM and VEEAM. Curriculum servers and the MIS (SIMS) server have Hardware Support under manufacture warranty and Software Support through our in-house ICT management team with 'next day' response for hardware failures. We have bespoke service contracts for SIMS, VMware, Smoothwall & Impero.

3.6 Backup routine

For all data stored on individual laptops (internal hard drives), it is the responsibility of the staff/pupil to backup data to ensure there is no data loss. All curriculum servers and the MIS server are backed up

All critical data is backed-up every 15 minutes via DPM. Additional we employ a GFS rotation system to ensure a off-site backup is maintained and a daily-weekly-monthly back-up to tape takes place.

3.7 Anti-Virus

All servers and network stations are covered by Microsoft Endpoint Protection Anti-Virus. Updates are downloaded daily and distributed to attached stations.

4. Managing the ICT infrastructure

4.1 Internet access, security and filtering

This academy:

- Has the educational filtered secure broadband connectivity through Virgin Media Business Broadband and so connects to the 'private' on-site firewall
- Uses the Smoothwall filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- Uses Impero user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the students
- Ensures network health through use of Microsoft Endpoint Protection anti-virus software and network set-up so staff and pupils cannot download executable files
- Uses DfE, LA approved systems such Egress Switch secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons
- Uses security timeouts on internet access where practicable/useful
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an ICT Acceptable Use Agreement form and understand that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment: the academy's learning environment
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the academy's Learning Platform as a key way to direct students to age/subject appropriate web sites; plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google Safe Search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- Informs all users that internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the system administrator/teacher/SLT. Our system administrator(s) logs or escalates as appropriate to the technical service provider
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse - through staff meetings and teaching programme

- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA

4.2 Network management (user access, backup)

This academy:

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses 'remote' management control tools for controlling workstations/viewing users/setting up applications and internet web sites, where useful (managed through Impero)
- Has additional local network auditing software installed (Impero)
- Storage of all data within the academy will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this academy:

- Ensures staff read and sign that they have understood the academy's E-safety Policy Suite. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different/use the same username and password for access to our academy's network
- Staff access to the academy's management information system (SIMS) is controlled through a separate password for data security purposes
- We provide pupils with an individual network log-in username. From Year 7 they are also expected to use a personal password
- All pupils have their own unique username and password which gives them access to the internet and the Learning Platform
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off/lock the workstation when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log off and then log on again as themselves
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day
- Has set up the network so that users cannot download executable files/programmes
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up to date and the academy provides them with a solution to do so
- Makes clear that staff accessing Trust systems do so in accordance with policies; e.g. finance system, personnel system etc.
- Maintains equipment to ensure Health and Safety is followed
- Has integrated curriculum and administration networks, but access to the Management Information System is set up so as to ensure staff users can only access modules related to their role; e.g. teachers access staff shared area; SEN coordinator - SEN data

- Ensures that access to the academy's network resources from remote locations by staff is restricted and access is only through academy VPN: e.g. teachers access their area/a staff shared area for planning documentation via a VPN solution
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child
- Provides pupils and staff with access to content and resources through the approved Learning Platform, which staff and pupils access using their username and password
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external audit requirements
- Uses our broadband network for our CCTV system and has been set up by approved partners
- Uses the DfE secure S2S website for all CTF files sent to other academies
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through S2S secure file exchange.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to industry standard enterprise security level/appropriate standards suitable for educational use
- Ensures all computer equipment is installed professionally and meets health and safety standards
- Ensures projectors are maintained so that the quality of presentation remains high
- Reviews the academy ICT systems regularly with regard to health and safety and security

4.3 Passwords

- Passwords for access to all academy systems must meet STRONG security criteria ensuring they are at least 7 characters long, include at least one upper case and one lower case letter, include at least one number and contain a special character
- This academy makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find
- All staff have their own unique username and private passwords to access academy systems. Staff are responsible for keeping their password private
- We require staff to change their passwords into the MIS/network, every 90 days (this is enforced through network software)

4.4 Email

All emails prepared and sent from this academy's email addresses and any non-work email sent using the academy's ICT facilities is subject to this section of the policy.

4.4.1 Email Risks

The academy recognises that there are risks associated with users accessing and handling information in order to conduct official academy business. This policy aims to mitigate the following risks:

- Failure to report information security incidents
- Inadequate destruction of data
- Loss of direct control of user access to information systems
- Exposure to legal action and/or adverse publicity
- Time wasting by inappropriate and unauthorised use
- Incorrect handling of CONFIDENTIAL information (see below)

If there are any questions or doubts about the category into which the information you are dealing with falls, then you should contact the Mr R Whitfield.

Non-compliance with this policy could have a significant effect on the efficient operation of the academy and may result in financial loss and an inability to provide necessary services to our customers.

4.4.2 Email as Records (Refer to Records Management and Archiving & Disposal Policies)

All emails that are used to conduct or support official academy business must be sent using an academy email address. Non-work email accounts **must not** be used to conduct or support official the academy business. Users must ensure that any emails containing sensitive information are sent from an official academy email. Any emails containing CONFIDENTIAL information must be marked as such and, when being sent externally, sent using WinZip encryption or via another approved encryption method. All emails that represent aspects of the academy business are the property of the academy and not of any individual employee.

Users should be aware any emails and attachments may need to be disclosed under the Data Protection Act or the Freedom of Information Act.

Emails held on the academy's equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any email message sent from a facility provided to conduct or support official academy business should be considered to be an official communication from the academy. In order to ensure that the academy is protected adequately from misuse of email, the following controls will be exercised:

- It is a condition of acceptance of this policy that users comply with the instructions given during the email training sessions.
- All official external email must carry the following disclaimer:
    - *"This document is strictly confidential and is intended only for use by the addressee. If you are not the intended recipient, any disclosure, copying, distribution or other action taken in reliance of the information contained in this email is strictly prohibited. Any views expressed by the sender of this message are not necessarily those of the academy. If you have received this transmission in error, please use the reply function to tell us and then permanently delete what you have received.*

      Please note: Incoming and outgoing email messages are routinely monitored for compliance with our policy on the use of electronic communications."
- External email signatures must follow the corporate standard and contain the following details:
    - Name
    - Post Title
    - Section
    - Department
    - Address
    - Telephone number
    - Email Address
    - Confidential disclosure

Whilst respecting the privacy of authorised users, the academy maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the academy's ICT systems.

4.4.3 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, or that the content will be understood in the way that the sender of the email intended. It is, therefore, the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or CONFIDENTIAL information or of communicating in the particular circumstances.

Email must not be considered to be any less formal than memos or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the academy's reputation or its relationship with parents/pupils, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the academy's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by the academy for email should not be used:

- For the transmission of:
  - Unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations
  - CONFIDENTIAL material concerning the activities of the academy to a third party
  - Material that this infringes the copyright of another person, including intellectual property rights unless required by law
- For activities that:
  - Unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users
  - Corrupt or destroy other users' data
  - Disrupt the work of other users
  - Violate the privacy of other users
- For the creation or transmission of:
  - Any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or defamatory material
  - Material which is designed or likely to cause annoyance, inconvenience or needless anxiety or material that is abusive or threatening to others, or serves to harass or bully others
  - Material that discriminates or encourages discrimination on grounds of race or ethnic origin, or on grounds of gender, sexual orientation, marital status, disability, and political or religious beliefs
  - Material which brings the academy into disrepute
  - Anonymous messages - i.e. without clear identification of the sender
- For so called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms
- For unfairly criticising individuals, including copy distribution to other individuals
- For disclosing to others any information given in documents classified with a protective marking without the prior consent of a person authorised to give it, unless under a requirement of law

- Printing off large volumes of personal emails and/or attachments using work printers unless arrangements have been made to reimburse the cost to the academy
- Reading, drafting and/or sending lengthy incoming and outgoing personal emails and/or attachments during working hours

Acceptable use of the academy email facility and addresses includes:
- Receiving small numbers of personal emails
- Printing off the occasional personal email and/or attachment using work printers
- Opening and identifying an email as being personal (once recognised as being personal the remainder of the email should not be read during working hours unless it is very short)
- Reading lengthy incoming personal emails and/or attachments outside of working hours
- Drafting and/or sending outgoing personal emails and/or attachments outside of working hours

Whilst employees have no control over incoming personal emails, they are responsible for ensuring these do not adversely impact on the academy email facility (in terms of quantity and size of attachments or by 'clogging up' individual mail boxes). Personal emails using academy facilities are subject to the same conditions as business use. For further guidance on what is acceptable and unacceptable use contact Mr R Whitfield.

4.4.4 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative email.

Before giving your email address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter emails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using the academy systems or facilities.

4.4.5 Mail Box Size

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of email addresses is discouraged.

Users are provided with a limited mail box size to reduce problems associated with server capacity. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 10mb in size.

4.4.6 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. Email is a business tool and as such can be audited and inspected without notice to users. The monitoring of email (outgoing and incoming) traffic will be undertaken so that the academy:

- Can plan and manage its resources effectively
- Ensures that users act only in accordance with policies and procedures
- Ensures that standards are maintained
- Can prevent and detect any crime
- Can investigate any unauthorised use

Monitoring of content will only be undertaken by staff specifically authorised for that purpose.

These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of email facilities
- Ensuring effective operation of email facilities
- Determining if communications are relevant to the business

Where an employee suspects that email facilities are being abused by a user, they should inform the Mr R Whitfield.

If any user is found to have breached this policy, they may be subject to the academy disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

4.4.7 Categorisation of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked with CONFIDENTIAL unless they are free to circulate publicly.

4.4.8 Security

Emails sent from the academy email system are held with the same network and are deemed to be secure. However, emails sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, CONFIDENTIAL material must not be sent via email outside this closed network, unless encryption is used (see Mr R Whitfield).

4.4.9 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure about whether they should pass on information, they should consult the Mr R Whitfield.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of the academy.

Care should be taken when addressing all emails, but particularly where they include CONFIDENTIAL information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent CONFIDENTIAL material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the Mr R Whitfield.

4.4.10 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must, therefore, be made of the academy's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to Mr R Smith.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus
- Must not download data or programs of any nature from unknown sources
- Must ensure that an effective anti-virus system is operating on any computer which they use to access academy facilities
- Must report any suspected files to Mr R Smith.

In addition, the academy will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the academy could be held liable if there has been negligence in allowing the virus to be transmitted.

4.4.11 Accessing Emails using Outlook Web Access

Currently, in order to access the Academy Outlook accounts remotely, the following actions are necessary (whether it be on a computer or smartphone):

1. Link to Microsoft office 365 sign in
2. Enter username and password
3. Select Outlook (Outlook web access)
4. Enter username and password again to access outlook
5. Read emails

There are now apps for smartphones that will automate steps 1 – 4 above.

Effectively, this means that the only security in place on smartphones to prevent unauthorised access to the academy email, if this app is used, is a 4-digit pin on the phone (provided one has been set up). For clarity, this means that if your phone is stolen, misplaced etc. and not locked, anyone would potentially have access to your email account and everything it contains.

All staff are therefore instructed that anyone accessing academy emails on smartphones **must setup a pin code security.**

This academy:

- provides staff with an email account for their professional use, and makes clear personal email should be through a separate account
- does not publish personal email addresses of pupils or staff on the academy website. We use anonymous or group email addresses, for example admin@academy.org or class email addresses (with one or more staff having access to a shared mailbox) for communication with the wider public
- will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law
- will ensure that email accounts are maintained and up to date
- reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police
- knows that spam, phishing and virus attachments can make emails dangerous

Pupils:

- are introduced to, and use email as part of the ICT/Computing scheme of work.
- are taught about the safety and 'netiquette' of using email both in the academy and at home i.e. they are taught:
    - not to give out their email address unless it is part of a an academy managed project or to someone they know and trust and is approved by their teacher or parent/carer
    - that an email is a form of publishing where the message should be clear, short and concise
    - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on academy headed paper
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
    - that they should think carefully before sending any attachments
    - that embedding adverts is not allowed
    - that they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature
    - not to respond to malicious or threatening messages
    - not to delete malicious of threatening emails, but to keep them as evidence of bullying
    - not to arrange to meet anyone they meet through email without having discussed with an adult and take a responsible adult with them
    - that forwarding 'chain' email letters is not permitted

- sign the ICT Acceptable Use Agreement to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- only use academy email systems for professional purposes
- access to external personal email accounts may be blocked in the academy
- use a 'closed' email system which is used for academy communications and some transfers of information
- never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect, etc.
- know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on academy headed paper. That it should follow the academy 'house-style'
- know sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
- know the sending of chain letters is not permitted
- know embedding adverts is not allowed
- sign our ICT Acceptable Use Agreement to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with

4.5 Academy website

- The Principal/Head of Academy takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained in line with Trust specifications and academy branding guidelines
- Uploading of information is restricted to our website authorisers
- The academy website complies with the statutory DfE guidelines for publications
- Most material is the academy's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the academy address, telephone number and we use a general email contact address, admin@kirkbalkacademy.org. Home information or individual email identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the academy website
- We do not use embedded geodata in respect of stored images
- We expect teachers using' academy approved blogs or wikis to password protect them and run from the academy website

4.6 Learning platform

- Uploading of information on the academy's Learning Platform/virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the academy's Learning Platform will only be accessible by members of the academy community
- In the academy, pupils are only able to upload and publish within academy approved and closed systems, such as the Learning Platform

4.7 Safeguarding from radicalisation (Refer to Preventing Radicalisation/Safeguarding Policy)

- The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our academy blocks inappropriate content, including extremist content
- The academy has safeguards in place to filter out radicalisation through social media, such as Facebook. Searches and web addresses are monitored and the ICT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found
- Where staff, students or visitors find unblocked extremist content they must report it to a senior member of staff
- We are aware that children and young people have access to unfiltered internet when using their mobile phones and staff are alert to the need for vigilance when pupils are using their phones
- Staff and students have a responsibility to report any instances of unblocked online searches or sharing of extremist messages or social profiles
- Any material that the academy believes is illegal will be reported to the appropriate agencies including the Police, CEOP and IWF
- For further guidance from the Home Office regarding how social media is used to encourage travel to Syria and Iraq please follow this link.

4.8 Social networking (Refer to Social Networking Policy)

- For their own security employees' should regularly review their privacy settings on all their social networking sites ensuring they have opted for the highest privacy settings on their account to minimise risks to themselves and the academy regarding reputation and professional integrity; however all communication via social networking sites should be made with the awareness that anything said,

shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore advised that staff follow the following procedures:

- Staff must not access social networking sites for personal use via Academy information systems or using Academy equipment.
- Staff must not accept students as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations.
- Staff are advised not to be friends with recent students. The potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking.
- Staff should not place inappropriate photographs on any social network space.
- Staff should not post indecent remarks.
- If a member of staff receives messages on his/her social networking profile that they think could be from a student they must report it to their Line Manager/Principal and contact the internet service or social networking provider so that they can investigate and take the appropriate action.
- Staff are advised not to write about their work, but where a member of staff chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the Academy. However, all other guidelines in this policy must be adhered to when making any reference to the workplace.
- Staff must not disclose any information that is confidential to the Academy or disclose personal data or information about any individual/colleague/student, which could be in breach of the Data Protection Act.
- Staff must not disclose any information about the Academy that is not yet in the public arena.
- In no circumstances should staff post photographs of students. The exception to this is if an employee's own child(ren) attend a NET academy. In these circumstances, it is accepted that images of their own children and their friends when at parties or such similar personal events may be posted. Care should be taken to ensure the suitability of the images. Images should not be posted in relation to the academy.
- Staff should not make defamatory remarks about the Academy /colleagues / students /parents or post anything that could potentially bring the Academy into disrepute.
- If inappropriate or defamatory comments are posted which may be construed as having potential to bring the academy, or an individual employed by the academy, into disrepute the employee must report it to the Principal immediately and the relevant procedure will be implemented. The employee may also need to contact the website involved, the GTC, their union or police
- Staff should not disclose confidential information relating to his/her employment at the Academy.
- Care should be taken to avoid using language which could be deemed as offensive to others.
- Where an academy uses social networking sites for communication purposes; e.g. it has its own Facebook page or Twitter account; these sites can be accessed via academy ICT equipment. However, this should be closely monitored and only those with administrator rights should communicate via these sites. Any misuse of the sites by staff, students, parents or the wider community should be reported immediately to the Principal.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the academy's preferred system for such communications (academy twitter account)
- Employees are reminded that information posted on social network sites could be visible to others who are not accepted friends on your account (e.g. posting a comment on a friend's wall on Facebook makes the information visible to all their friends; if you are 'tagged' on a friend's photo album the whole album is visible to their friends, your friends and anyone else tagged in the same album). Exercise caution with information written and photographs displayed by you and others and make friends aware of implications on your professional integrity.

Breaches of the Policy

- The Governing Body does not discourage staff from using social networking sites. However, all staff should be aware that the Trust and the Governing Body will take seriously any occasions where the services are used inappropriately. If occasions arise of what could be deemed to be online bullying or harassment, these will be dealt with in the same way as other such instances.
- Any use of social network sites on the academy network will be monitored using relevant software. If any instances of the inappropriate use of social networking sites are brought to the attention of the Principal, depending on the seriousness of the allegations, disciplinary action may be taken.
- There may be instances where the Academy will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality.

4.9 CCTV (Refer to CCTV Policy)

- We have CCTV in the academy as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission, except where disclosed to the Police as part of a criminal investigation
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes

4.10 Biometrics

This academy:

- Ensures that the pupils' biometric data is treated with appropriate care and complies with the data protection principles as set out in the Data Protection Act 1998
- Ensures, that where data is to be used as part of an automated biometric recognition system, that it complies with the additional requirement in sections 26 to 28 of the Protection of Freedoms Act 2012
- Ensures that each parent/child is informed about the use of the biometric systems at the academy (see Appendix 3 - Privacy Notices)
- Ensures that at least one parent has given written consent before data is taken to be used with any biometric system
- Provides reasonable alternatives of accessing services for those pupils who have opted out of using the system
- Ensures that all biometric data that is stored is encrypted
- Ensures that all biometric data is erased when a pupil leaves the academy
- Has systems in place that allow parents to withdraw their consent at any time (must be in writing in the form of a letter or email)

4.11 VPN (Remote Access)

The academy provides users with the facilities and opportunities to work remotely as appropriate to their role. The academy will ensure that all users, who work remotely, are aware of the acceptable use of portable computer devices and remote working opportunities.

Portable computing devices are provided to assist users to conduct official academy business efficiently and effectively. This equipment, and any information stored on it, should be recognised as valuable organisational information assets and safeguarded appropriately.

This section of the policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of the academy IT equipment and personal IT equipment when working on official academy business away from the academy premises (i.e. working

remotely). This policy also applies to all users' use of the academy IT equipment and personal IT equipment to access academy information systems or information whilst outside the United Kingdom.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers
- Tablet PCs
- PDAs
- Palm pilot
- Mobile phones
- Text pagers
- Wireless technologies

4.11.1 Risk

The academy recognises that there are risks associated with users accessing and handling information in order to conduct official academy business. The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves.

Securing CONFIDENTIAL information when users work remotely or beyond the academy network is a pressing issue – particularly in relation to the academy's need as an organisation to protect data in line with the requirements of the Data Protection Act 1998.

This aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft
- Wider use of mobile IT equipment where personal or sensitive data may be stored
- Accidental or deliberate overlooking by unauthorised individuals
- Unauthorised access to CONFIDENTIAL information
- Exposure of personal and sensitive client information
- Unauthorised introduction of malicious software and viruses
- Potential sanctions against the academy or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse
- Potential legal action against the academy or individuals as a result of information loss or misuse
- Academy reputational damage as a result of information loss or misuse

Non-compliance with this policy could have a significant effect on the efficient operation of the academy and may result in financial loss and an inability to provide necessary services to our customers, as well as exposing sensitive and/or personal client data to unauthorised users/environments.

4.11.2 User Responsibility

This academy:

- Ensures all IT equipment used to access the VPN (including portable computer devices) is supplied to users and is the property of Kirk Balk Academy. It must be returned upon the request of Kirk Balk Academy. Access for ICT Services staff of Kirk Balk Academy shall be given to allow essential maintenance security work or removal, upon request
- Ensures ICT Services will deploy an up-to-date anti-virus signature file to all users who work away from the Kirk Balk Academy premises
- Ensures remote users' access to academy systems (if connecting over public networks, such as the Internet) need to be via VPN. No other access routes can be used
- Ensures users are made aware of the physical security dangers and risks associated with working within any remote office or mobile working location
- Ensures that the users are made aware that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site
- Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every week (unless valid reasons why this cannot be achieved, e.g. sickness) to enable the anti-virus software to be updated
- Users will not install any hardware to or inside any academy owned portable computer device, unless authorised by Mr R Whitfield.
- Users will allow the installation and maintenance of hardware/software by the In-house IT support team
- Users will inform the IT Helpdesk (3rd party IT provider) of any academy owned portable computer device message relating to configuration changes
- Business critical data should be stored on an academy file and print server wherever possible and not held on the portable computer device
- Passwords and/or other access information should not be written down and stored near the portable device
- All mobile devices (e.g. laptops and tablet PCs) must be locked with a password that uses the VPN
- Personal or sensitive documents can only be stored temporarily onto encrypted devices (if you have no access to the academy's network). If such information must be stored because there is no access to the network, then the number of records/cases must be kept to a minimum
- Any personal or sensitive documents saved temporarily on laptop hard drives/pen drives must be copied to the academy network and then removed from the hard drive/pen drive as soon as you can access the network. Personal or sensitive documents must not be allowed to remain on mobile devices. Also pen drives/external drives must be encrypted (See removable media section)
- If you wish to work from home on personal or sensitive documents, you should only do so by using the secure academy network (where no documents are saved to the PC/laptop)
- If you take an academy laptop home with you, it should be stored in a secure location and you must make sure that it is not left in your car etc.
- The user shall ensure that appropriate security measures are taken to stop unauthorized access to CONFIDENTIAL information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as Kirk Balk Academy itself
- All faults must be reported to the IT Helpdesk
- Users must not remove or deface any asset registration number and only those devices with an asset number/tag can be connected to the academy network
- User requests for upgrades of hardware or software must be approved by the Network Manager & Line manager. Equipment and software will then be purchased and installed by IT Services
- Personal use of the IT equipment by staff is allowed outside of working hours. However, this policy and acceptable use must be fully adhered to. In particular, the equipment must not be used in relation to running an external business and websites containing illegal, unsuitable and inappropriate material, must not be accessed. Only software supplied and approved by Kirk Balk Academy can be used (e.g. Word, Excel, Adobe, etc.). The IT equipment is supplied for the employee's sole use and nobody else, including family members, must use it
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Kirk Balk Academy may recover the costs of repair (calculated at a pre-determined rate). This charge is subject to annual review
- The user should seek advice from the Mr R Whitfield before taking any academy supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the academy's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel
- Kirk Balk Academy may at any time, and without notice, request a software or hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database, or carry out any processing of CONFIDENTIAL information relating to the academy, its employees, or pupils/parents. **Under no circumstances** should personal or CONFIDENTIAL information be emailed to a private non-academy email address. For further information, please refer to the Email section of this policy

4.11.3 Anti-virus Protection

ICT Services (through the academy and/or 3rd party IT provider) will deploy an up to date anti-virus signature file to all users who work away from the academy premises. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every week (unless valid reasons why this cannot be achieved, e.g. sickness) to enable the anti-virus software to be updated.

If any user has any doubt as to what is or is not acceptable use of mobile devices, they should contact Mr R Whitfield

5. Security

5.1 Data security: Management Information System access and data transfer

Strategic and Operational Practices (see Data Protection Policy, Data Security Breach Policy and Information Security and Assurance Policy)
At this academy:

- the Principal is the Senior Information Risk Officer (SIRO)
- we ensure staff know to whom to report any incidents where data protection may have been compromised (Mr R Whitfield – Acting Vice Principal)
- all staff are DBS checked and records are held in one central record
- we ensure ALL the following academy stakeholders sign an ICT Acceptable Use Agreement. We have a system so we know who has signed
  - Staff
  - Governors
  - Pupils
  - Parents
  - Guests

  This makes clear staffs' responsibilities with regard to data security, passwords and access
- we follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services
- we require that any Protect and Restricted material must be encrypted if the material is to be removed from the academy and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home (VPN)
- academy staff with access to setting up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems
- we ask staff to undertake at least annual housekeeping to review, remove and destroy any digital materials and documents, which need no longer be stored
- students and staff will be given a Privacy Notice (see Appendix 3) annually which informs them how the data held in the academy is treated and protected. The parent of the student or the member of staff will be required to sign this notice to confirm they are happy with the academy procedures for handling data.

5.2 Technical Solutions

- Staff have a secure area(s) on the network to store sensitive documents or photographs
- We require staff to logout of systems when leaving their computer, but also enforce lockout after a given time period
- We use encrypted flash drives if any member of staff has to take any sensitive information off site
- We use the DfE S2S site to securely transfer CTF pupil data files to other academies

- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area
- All servers are in lockable locations and managed by Mr R Smith – Network Manager
- We lock any backup tapes in a secure, fire-proof cabinet. Backups are encrypted
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment, where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data
- Portable equipment loaned by the academy (for use by staff at home), where used for any protected data, is disposed of through the same procedure
- Paper based sensitive information is shredded, using cross cut shredder/collected by secure data disposal service
- We are using secure file deletion software through Microsoft DPM

5.3 Removable Media

The academy will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official academy business. This policy should be adhered to at all times, but specifically whenever any user intends to store information used by the academy to conduct official business on removable media devices.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required
- Maintain the integrity of the data
- Prevent unintended or deliberate consequences to the stability of the academy's computer network
- Avoid contravention of any legislation, policies or good practice requirements
- Build confidence and trust in the data that is being shared between systems
- Maintain high standards of care in ensuring the security of protected and restricted information
- Prohibit the disclosure of information as may be necessary by law

Removable media devices include, but are not limited to the following:

- CDs
- DVDs
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Digital Cameras/memory cards

5.3.1 Risks

The academy recognises that there are risks associated with users accessing and handling information in order to conduct official academy business. Information is used throughout the academy and sometimes shared with external organisations and applicants. Securing CONFIDENTIAL data is of paramount importance – particularly in relation to the academy's need to protect data in line with the requirements of the Data Protection Act 1998.

Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the academy. It is therefore essential for the continued operation of the academy that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the academy's needs.

This policy aims to mitigate the following risks:

- Disclosure of CONFIDENTIAL information as a consequence of loss, theft or careless use of removable media devices
- Contamination of academy networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another
- Potential sanctions against the academy or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse
- Potential legal action against the academy or individuals as a result of information loss or misuse
- Academy reputational damage as a result of information loss or misuse

5.3.2 Restricted Access to Removable Media

It is the academy policy to discourage the use of removable media as far as reasonably practicable for the transfer of confidential information. Where there is no practicable alternative then removable media may be used only when agreed by the Mr R Whitfield There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

5.3.3 Encryption of Removable Media

All USB memory sticks and external hard drive devices which are used to transport personal/sensitive data must have encryption activated on them and **must only** be used with academy owned or leased IT equipment.

All removable media must be approved by the academy (whoever holds responsibility for ICT) to ensure the level of encryption is adequate

5.3.4 Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment, than data which is frequently backed up. Therefore, removable media should not be the only place where data obtained for academy purposes is held. Copies of any data stored on removable media must also remain on the source system or network until the data is successfully transferred back to the network or system. Data stored on removable media must only be done so temporarily and removed at the earliest opportunity. Data should not be permanently held on a removable media device.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. All data stored on removable media must be stored on encrypted removable media devices.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

For further information on information security please refer to the policies listed below, which are all available on the NET Portal:

- Information Security and Assurance Policy
- Information Strategy
- Data Protection Policy
- Data Security Breach Policy
- Publication Scheme
- Records Management Policy

5.3.5 Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to their line manager and Mr R Whitfield who will then inform the Trust Head Office. It is the duty of all employees to report any actual or suspected breaches in information security to the Principal. Please refer to the academy's Critical Incident Management Plan to manage any incidents.

5.3.6 Third Party Access to Academy Information

No third party (external contractors, partners, agents, the public or non-employee parties) may extract information from the academy network information stores or IT equipment and place on a removable media device without explicit agreement by the Principal.

Should third parties be allowed access to academy information then all the considerations of this policy apply to their storing and transferring of the data.

5.3.7 Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to stop using removable media when it is damaged and report it to the ICT Lead who will arrange for its safe disposal.

Academy information must only be transferred on/between removable devices provided by the academy to ensure the risk from viruses or other security threats is minimised and the correct level of encryption is applied.

Virus and malware checking software approved by the academy's IT providers must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned before the media is loaded on to the receiving machine.

Whilst in transit or storage the data held must be on an encrypted device to reduce risk to the academy, other organisations or individuals from the data being lost whilst in transit or storage.

5.3.8 Disposing of Removable Media Devices

Removable media devices, that are no longer required or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to the Network Manager for disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the ICT lead.

5.3.9 User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with academy equipment or the network or to hold information used to conduct official academy business **must** be checked for viruses/malware before use
- All data stored on removable media devices **must** only be stored on encrypted devices.
- Virus and malware checking software **must** be used when the removable media device is connected to a machine
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved
- Removable media devices **must not** to be used for archiving or storing records as an alternative to other storage equipment
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss
- A record of the information placed onto any removable media device **must** be kept by the user and be available to the academy
- Information held on a removable media device must be kept to a minimum
- All information should be removed from the removable media device and placed onto the academy networked system as soon as available

For advice or assistance on how to securely use removable media devices, or for further advice or clarification on any part of this policy, please contact the Mr R Whitfield.

5.3.10 Key Messages

The key messages within this section are summarised below:-

- It is the academy policy to limit the use of all removable media devices to transport confidential data
- Any removable media device used for confidential data **must be** encrypted
- Damaged or faulty removable media devices must not be used to store confidential data and should be reported and destroyed securely
- Special care **must be** taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage

6. Equipment and Digital Content

6.1 Personal mobile phones and mobile devices

- Mobile phones brought into the academy are entirely at the staff member's, student's, parent's or visitor's own risk. The academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into the academy

- Student mobile phones which are brought into the academy must be turned off (not placed on silent) and stored out of sight on arrival at the academy. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during academy break times. All visitors are requested to keep their phones on silent
- Smart devices (including Smart watches) must be turned off (not placed on silent) and stored out of sight on arrival at the academy
- Students with Smart watches must remove them before entering an exam. Smart devices must not be taken into exams under any circumstances. Exceptions will only be made if the device is needed for the exam and will require prior authorisation
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Principal. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary
- The academy reserves the right to search the content of any mobile or handheld device on the academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the academy site, e.g. changing rooms and toilets
- Mobile phones will not be used during lessons or formal academy time unless as part of an approved and directed curriculum-based activity with consent from a member of staff
- The Bluetooth or similar function of a mobile phone should be hidden or switched off at all times and not be used to send images or files to other mobile phones. If not hidden/switched off it is visible to others and there is no control over the information that is sent/received
- No images or videos should be taken on mobile phones or personally owned mobile devices without the prior consent of the person or people concerned

6.2 Students' use of personal devices

- The academy accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety
- If a student breaches the academy policy then the phone or device will be confiscated and will be held in a secure place in the academy office. Mobile phones and devices will be released to parents or carers in accordance with the academy policy
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- If a student needs to contact his or her parents or carers, they will be allowed to use an academy phone. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy office
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

6.3Staff use of personal devices

- Any permitted images or files taken in the academy must be downloaded from the device and deleted in the academy before the end of the day (not to be taken home)
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances
- If a member of staff breaches the academy policy then disciplinary action may be taken

Staff using personally owned mobile phones for work use:

- Are subject to audit checks if mobile expenses claims are submitted

- Must ensure the mobile device is pin code/password protected at all times with a screen lock
- Must not allow another person to access their mobile device for any reason to ensure there is no risk to any sensitive data stored on the device
- Must ensure remote deletion of data is setup in case the device is lost or stolen (e.g. Apple's 'Find iPhone')
- Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during offsite activities, or for contacting students or parents, then an academy mobile phone will be provided and used. Where a staff member doesn't have access to an academy-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes

Digital Images and Video in this Academy

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the academy agreement form when their daughter/son joins the academy
- Staff sign the academy's ICT Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils
- Images of students should not be stored on any personal mobile device. Images taken using academy mobile devices must not be removed from academy premises without authorisation from the Vice Principal/Principal
- If specific pupil photos (not group photos) are used on the academy website, in the prospectus or in other high profile publications the academy will obtain individual parental or pupil permission for its long term use
- All images and videos will be analysed by academy security software. If there is a suspicion they are inappropriate they will be recorded for nominated staff to review and take action, if necessary
- The academy blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Photos or videos which include nudity or inappropriate actions are not permitted to be taken, downloaded, viewed or stored under any circumstance on academy ICT equipment or the network.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or academy. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse

6.4 Asset disposal

- Details of all academy owned hardware will be recorded in a hardware inventory
- Details of all academy owned software will be recorded in a software inventory
- All redundant 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 equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The academy will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website

7.0 Appendices

Appendix 1	ICT Acceptable Use Agreements
Appendix 2	Academy E-safety Audit Template
Appendix 3	Privacy Notices
Appendix 4	E-safety useful links and resources
Appendix 5	Incident response flowchart and log
Appendix 6	Legal framework

APPENDIX 1

ICT ACCEPTABLE USE AGREEMENT (STAFF)

Introduction

Northern Education Trust (NET) is committed to ensuring that all employees, students and other users are aware of their responsibilities regarding use of ICT equipment, software, and the ICT networks.

Responsibility for this policy rests with the Governing Body and the Senior Leadership Team. Responsibility for compliance to this policy rests with the individual user. It applies to all users of the ICT systems including 'Guests'.

The use of ICT facilities within the academy is encouraged, as its appropriate use facilitates communication and can improve efficiency. Used correctly, it is a valuable tool for employees and students. Inappropriate use, however, causes problems ranging from minor distractions to exposing the academy to financial, technical, commercial and legal risks.

Our ICT Acceptable Use Agreement has been created as a reference guide to ensure the academy network is operated safely and users are safeguarded. It relates to academy ICT facilities and acceptable and unacceptable use.

For more detailed information, staff are requested to read through each of the sections covered within this E-Safety Policy Suite.

Responsibility to comply with the policy at all times rests with the user. Regular monitoring systems are in place to inform SLT of inappropriate use. Non-compliance with the policy could initiate disciplinary procedures such as:

- Temporary or permanent withdrawal from the academy system
- Suspension or exclusion from the academy
- Disciplinary action which could lead to dismissal
- In the most serious cases legal action may also be taken

Network Protocol

- The academy network and associated services may be used for lawful purposes only. This includes no copying, recording or distribution of any illegal material such as television media, films, telephone conversations and music. Permission should be sought if the user is unsure if it is legal to do so
- Network and internet use must be appropriate to a student's education or to employee professional activity. If unsure about your required use, please seek authorisation from Mr R Whitfield.
- Users must not misuse or waste IT resources, particularly printer ink, toner and paper and network traffic (e.g. sending lots of printing to a printer)
- Users, who require a large print job of more than 30 sheets, should refer to reprographics

- Users may access IT facilities for personal use during break/lunch times provided it does not interfere with their academy responsibilities and does not contravene the ICT usage rules outlined in this document
- Use of the academy network will be supervised by key logging security software and will monitor all activity, recording any inappropriate language or use, e.g. chat rooms, internet use, typing and file names etc.
- The SLT and the Managed Service provider can remotely view any of the computers on the network. This may be used randomly to implement the ICT Policy and to assist with any user difficulties
- Users must ensure that employee/student related information is not stored within shared areas
- Users should ensure their files/folders are structured within their account in an efficient manner to utilise space on the network

Passwords

- Each student or employee must log on using their own user name and password. Users must not attempt to use someone else's network account
- When equipment is left unattended, you must log off or a password protected screen saver must be activated
- Any supply teachers or visitors must log onto the system as a Guest only and a record will be kept of who is using each unique Guest password
  Students, employees or visitors must not give their password or user account details to anyone. This comes under the Computer Misuse Act and is illegal. If your password is lost or someone discovers your password you must inform Mr R Whitfield. Passwords must be changed at regular intervals

Hardware, Software and Downloads

- Users must not install hardware devices including USB devices onto the network without permission from Mr R Whitfield who will advise of necessary virus check routines
- Users must not install software onto the network without permission from the Managed Service provider
- Copyright and intellectual property rights must be respected when downloading from the internet
- Users must not undertake any form of piracy including the infringement of software licences or other copyright provisions whether knowingly or not. This is illegal
- Users must not purchase any IT facilities without the consent of Mr R Whitfield This is in addition to any purchasing arrangements followed according to Trust financial regulations
- Users must not knowingly distribute or introduce a virus or harmful code onto the academy's network or equipment. Doing so could lead to action by the academy outlined in the introduction
- Users must not relocate, take off-site or otherwise interfere with the IT facilities without the authorisation of Mr R Whitfield
- If students/employees wish to loan IT equipment for use away from academy premises please see Mr R Whitfield to grant permission for the loan and record it in the log
- Users must not misuse or damage IT related equipment
- Equipment loaned to a member of staff is for their sole use and is not to be used by friends/family members due to the ability to remote access confidential data. Equipment will be monitored for misuse and damage and therefore must only be used by the named individual

Data/Removable Media (See Data Protection Policy & Data Security Breach Policy)

- Student and employee data is stored in line with Data Protection requirements
- Any student/employee related data must be stored securely if taken off site (with appropriate data encryption - please see …….. for advice on how this can be done)).
- Student/employee data must not be accessed for personal use
- It is Kirk Balk Academy policy to limit the use of all removable media devices to transport confidential data
- Any removable media device used for confidential data must be encrypted
- Damaged or faulty removable media devices must not be used to store confidential data and devices that have become damaged, must be disposed of securely to avoid data leakage

- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices must only be used for data transport, not for permanent storage
- Information held on a removable media device must be kept to a minimum
- Ensure you are familiar with the academy Information Security polices which can be found on the NET Portal:
  - Information Strategy
  - Information Security and Assurance Policy
  - Data Protection Policy
  - Data Security Breach Policy
  - Publication Scheme
  - Records Management Policy

Academy Email System

- All emails that are used to conduct or support official Kirk Balk Academy business must be sent using a "@kirkbalkacademy.org" address.
- Non-work email accounts must not be used to conduct or support official Kirk Balk Academy business
- Users must ensure that any emails containing sensitive information are encrypted and must be sent from an official academy email
- All official external email must carry the official Kirk Balk Academy disclaimer and a signature which follows the corporate standard (see section 4.4.2 NET E-safety Policy Suite)
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the academy's Equal Opportunities policy
- Forwarding should be limited to an alternative academy email which is monitored by someone appropriate for the content which may be delivered.
- It is unacceptable to setup forwarding to a personal email account due to the risk of a Data Protection breach
- Emails should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent
- Email attachments should only be opened if the source is known and trusted
- Students are not permitted under any circumstances to email a member of staff's personal email
- Students must never provide their personal details online (such as name, address, age or telephone number)
- Academy email should not be used for personal correspondence
- Users must ensure that all necessary steps are taken to protect confidential emails. The academy will be liable for any defamatory information circulated either within the academy or to external contacts
- The academy email system and accounts must never be registered or subscribed to SPAM
- Any unsuitable emails received must be reported to Mr R Whitfield immediately
- Offers or contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between you or the academy and the recipient. Never commit the academy to any obligations by email or the internet without ensuring that you have the authority to do so. If you have any concerns contact the SLT.
- All emails sent and received will be recorded for a time period of no less than six months
- If employees access academy email off site they must use the web access facility or access it via a secure encrypted academy device
- Employee use of personal email accounts is only permitted if they have built-in anti-virus protection approved by the academy. Access to your personal email is allowed during break/lunch times provided it does not interfere with your academy related responsibilities and does not contravene the ICT usage rules outlined in this document or other policy documentation.
- All staff are therefore instructed that anyone accessing academy emails on Smartphones **must setup a pin code security**

Images/videos

- All students may have photographs taken or videos made in line with academy requirements unless parents indicate they do not authorise this
- Photos or videos which include nudity or inappropriate actions are not permitted to be taken, downloaded, viewed or stored under any circumstance on academy ICT equipment or the network
- All images and videos will be analysed by academy security software. Inappropriate use will be recorded for nominated staff to review and take action if necessary
- Images of students must not be posted on staff personal social networking sites

Internet Usage

- Students must be supervised where possible when using the internet
- Use of all internet sites will be recorded and analysed for nominated staff to review and take action if necessary
- Use of the internet for personal financial gain, gambling, political purposes, advertising or illegal activity is forbidden
- Staff and students have a responsibility to report any instances of witnessing or discovering blocked online searches or sharing of extremist or bullying messages or social profiles.
- Any material/activity that the academy believes is illegal will be reported to the appropriate agencies including the Police, Child Exploitation and Online Protection Centre (CEOP) and Internet Watch Foundation (IWF).

Internal Phone/Postal System

- Telephone and postal system use must be appropriate to a student's education or to staff professional activity. If you are unsure about your required use, please seek authorisation from your line manager
- Staff use of the academy's telephone facilities for personal use is permitted for necessary UK calls lasting less than 10 minutes so long as this does not interfere with your job role duties. If you need to use the telephone for longer than this or you need to make a call overseas, authorisation must be sought first from the SLT on each occasion and they should be notified immediately after the call. Any personal use of the telephones is at the Principal's discretion and should fall within reasonable usage
- Users must not re-locate, take offsite or otherwise interfere with the telephone system facilities without the authorisation of the SLT
- Users must not utilise the academy phone/post facilities to access, receive, view or display any of the following:
    - Any material that is illegal
    - Any material that could constitute bullying or harassment or any negative comment about other persons or organisations
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit material
    - Any adult or chat line phone numbers.
- All users are prohibited from attempting to use the academy's phone/post facilities to undertake ANY form of piracy including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal
- Users must not copy, record or distribute any material from or with the academy phone/post facilities that may be illegal to do so. This can include television media, films, telephone conversations and music. If you are unsure if you have permission to do this please see Mr R Whitfield.

Mobile devices

- Employee personal mobile phones/devices must not be connected to the academy data/internet network but can be connected to the Guest internet connection
- Employees are advised to security lock their mobile phones when left unattended

- Images of students should not be taken/stored on any personal mobile device. Images taken using academy mobile devices must not be removed from academy premises without authorisation from the Principal
- Students are allowed to use their mobile devices on academy property for teaching and learning purposes only and in line with instructions given from teaching staff
- Any Student or Employee data must be saved on the network drive, not the internal drive of any mobile device (i.e. Teacher Laptops)
- Any personal use of mobile devices is at the Principal's discretion and should fall within reasonable usage.

Social Networking (Refer to Social Networking Policy)

- For their own security employees' should regularly review their privacy settings on all their social networking sites ensuring they have opted for the highest privacy settings on their account to minimise risks to themselves and the academy regarding reputation and professional integrity; however all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore advised that staff follow the following procedures:
    - Staff must not access social networking sites for personal use via academy information systems or using academy equipment.
    - Staff must not accept students as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations.
    - Staff are advised not to be friends with recent students. The potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking.
    - Staff should not place inappropriate photographs on any social network space.
    - Staff should not post indecent remarks.
    - If a member of staff receives messages on his/her social networking profile that they think could be from a student they must report it to their Line Manager/Principal and contact the internet service or social networking provider so that they can investigate and take the appropriate action.
    - Staff are advised not to write about their work, but where a member of staff chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the academy. However, all other guidelines in this policy must be adhered to when making any reference to the workplace.
    - Staff must not disclose any information that is confidential to the academy or disclose personal data or information about any individual/colleague/student, which could be in breach of the Data Protection Act.
    - Staff must not disclose any information about the academy that is not yet in the public arena.
    - In no circumstances should staff post photographs of students. The exception to this is if an employee's own child(ren) attend a NET academy. In these circumstances, it is accepted that images of their own children and their friends when at parties or such similar personal events may be posted. Care should be taken to ensure the suitability of the images. Images should not be posted in relation to the academy.
    - Staff should not make defamatory remarks about the academy /colleagues / students /parents or post anything that could potentially bring the academy into disrepute.
    - If inappropriate or defamatory comments are posted which may be construed as having potential to bring the academy, or an individual employed by the academy, into disrepute the employee must report it to the Principal immediately and the relevant procedure will be implemented. The employee may also need to contact the website involved, the GTC, their union or police
    - Staff should not disclose confidential information relating to his/her employment at the academy.
    - Care should be taken to avoid using language which could be deemed as offensive to others.
    - Where an academy uses social networking sites for communication purposes; e.g. it has its own Facebook page or Twitter account; these sites can be accessed via academy ICT equipment. However, this should be closely monitored and only those with administrator rights should

communicate via these sites. Any misuse of the sites by staff, students, parents or the wider community should be reported immediately to the Principal.

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the academy's preferred system for such communications (academy twitter account)
- Employees are reminded that information posted on social network sites could be visible to others who are not accepted friends on your account (e.g. posting a comment on a friend's wall on Facebook makes the information visible to all their friends; if you are 'tagged' on a friend's photo album the whole album is visible to their friends, your friends and anyone else tagged in the same album). Exercise caution with information written and photographs displayed by you and others and make friends aware of implications on your professional integrity.

Breaches of the Policy

- The Governing Body does not discourage staff from using social networking sites. However, all staff should be aware that the Trust and the Governing Body will take seriously any occasions where the services are used inappropriately. If occasions arise of what could be deemed to be online bullying or harassment, these will be dealt with in the same way as other such instances.
- Any use of social network sites on the academy network will be monitored using relevant software. If any instances of the inappropriate use of social networking sites are brought to the attention of the Principal, depending on the seriousness of the allegations, disciplinary action may be taken.
- There may be instances where the academy will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality.

Remote Access

- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software that has not been approved, taking due care and attention when transporting and storing the equipment and not emailing CONFIDENTIAL information to a non-academy email address
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location
- It is the user's responsibility to ensure that access to all CONFIDENTIAL information is controlled – e.g. through password controls
- All CONFIDENTIAL data held on portable computer devices must be encrypted **(saved to the academy network, not to the local drive)**

Reporting Incidents

- Employees are required to inform Mr R Whitfield immediately of any abuse of the academy ICT systems
- Students are required to inform a member of staff immediately of any abuse of the academy ICT systems

Declaration

I hereby declare that I have read and understood the ICT Acceptable Use Reference Guide above, and the policy suite it refers to, and as an employee of Northern Education Trust I will abide by the regulations set out in this document.

Name: …… Date: ……

Signature ……..

Once signed this ICT Acceptable Use Agreement (Staff) should be photocopied, the original must be filed in the individuals personnel file with the copy being held by the individual for reference.

ICT ACCEPTABLE USE AGREEMENT (STUDENT)

Please find a summary of our ICT Acceptable Use Agreement printed below. Please discuss the following rules with your child. If you agree to them please sign and date this form below and return to the academy.

All computers within the academy have Internet access to help our learning and these rules will keep everyone safe and help us to be fair to others.

- I will only access the network and other ICT systems using my own login details, which I will keep secret.
- I will not access other people's files.
- I will only use the computers for schoolwork and homework.
- I will not bring in USB pens from outside the academy unless I have been given permission.
- I will ask permission from a member of staff before using the Internet and will always work so that the member of staff can see my computer monitor screen.
- I will only e-mail people that my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give out my personal details (date of birth, home address, telephone number, etc.) on the internet or by email
- I will report any unpleasant material or messages sent to me. I understand that my report would be confidential and would help protect other students and myself.
- I understand that the academy may check my computer files and may monitor the Internet sites I visit.
- I must not copy, record or distribute any material from or with the academy network facilities that may be illegal to do so. This can include television media, films, telephone conversations and music
- I understand that the academy network will be supervised by key logging security software and will monitor all activity, recording any inappropriate language or use, e.g. chat rooms, internet use, typing and file names etc.
- I must not knowingly distribute or introduce a virus or harmful code onto the academy's network or equipment.
- I must not misuse or damage IT related equipment.
- I understand that any use of social network sites on the academy network will be monitored using relevant software. If there is a suspicion of anything inappropriate, information will be recorded for nominated staff to review and take action if necessary.
- I will ensure that my files/folders are structured within my account in an efficient manner to utilise space on the academy network.
- I understand that the use of personal mobile devices on academy property is for teaching and learning purposes only, and in line with instructions given from teaching staff.

Name of Student _____ Year Group _____

Student Signature _____

Date _____

To the Parent / Carer

I have read the ICT Acceptable Use Agreement of the academy and as a parent or legal carer of the student named above, I grant permission for my child to use the networked computer systems, electronic mail and the Internet. I understand that students will be held accountable for their own actions and acknowledge that anyone abusing the system, either on the academy network or the internet, will have their access rights terminated. I will contact the Principal if I no longer wish my child to use the academy network with access to the Internet.

Name of Parent / Carer _____

Signature _____

Date _____

Once signed this ICT Acceptable Use Agreement (Student) should be photocopied, the original must be filed in the student file with the copy being held by the student for reference.

ICT ACCEPTABLE USE AGREEMENT (GUEST)

Academy networked resources, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the academy. If you make a comment about the academy or The Trust you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the academy or the Trust into disrepute is not permitted.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions will lead to withdrawal of the user's access; monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution.

Personal Responsibility

Users are responsible for their behaviour and communications. Guests will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Network Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the academy code of conduct.

- I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the academy or Northern Education Trust into disrepute.
- I will use appropriate language. Illegal activities of any kind are strictly forbidden.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I understand that users under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
- Privacy – I will not reveal any personal information (e.g. home address, telephone number, 5 social networking details, and medical data) of other users to any unauthorised person. I will not reveal any of my personal information to students.
- I will not trespass into other users' files or folders unless necessary in order to conduct the task that I have been employed to do.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
- I will ensure that if I think someone has knowledge my password then I will change it immediately and/or contact the Network Manager.
- I will ensure that I log off after my network session has finished.
- If I find an unattended machine logged on under other users username I will not continuing using the machine – I will log it off immediately.
- I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the academy leadership team.
- I will not use the network in any way that would disrupt use of the network by others.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the Network Manager.
- I will not use "USB drives", portable hard-drives, "floppy disks" or personal laptops on the network without having them "approved" by the academy checked for viruses.
- I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

- I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
- I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such as academy parents and their children.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
- I will support and promote the academy's e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
- I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on the SIMS database.
- I will not receive, send or publish material that violates copyright law.
- I will not attempt to harm or destroy any equipment or data of another user or network connected to the academy system.
- I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

Network Security

Users are expected to inform the Network Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Users identified as a security risk will be denied access to the network.

Media Publications

No media is to be copied or removed from the academy Network.

ICT Acceptable Use Agreement (Guest) Declaration

As an academy user of the network resources, I agree to follow the academy rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the ICT Acceptable Use Agreement. If I am in any doubt I will consult the Network Manager.

I agree to report any misuse of the network to the Network Manager. I also agree to report any websites that are available on the academy Internet that contain inappropriate material to the Network Manager.

Any information contained within the data I access is strictly confidential and will not be revealed to any persons

If I do not follow the rules, I understand that this may result in criminal prosecution. I realise that guests under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Guest Name: _____

Guest Signature: _____ Date: _____

Once signed this ICT Acceptable Use Agreement (Guest) should be photocopied, the original must be filed in the office with the copy being held by the guest for reference.

Academy E-safety Audit

Please complete the Network/E-safety Quick Audit Checklist below annually. Any gaps uncovered by this audit should inform your ICT Development Plan

No.	Summary points	Tick
1.	All staff/students/Governors/visitors sign and understand the ICT Acceptable Use Agreement	
2.	One parent has given written consent before data is taken to be used with any biometric system	
3.	Network monitoring software is active across the network (e.g. securus)	
4.	Each user of the network must have their own unique login (No shared logins)	
5.	All redundant Students/Staff/Visitors accounts must be deactivated or deleted	
6.	Users that use Guest accounts must be recorded (name and date accessed etc.)	
7.	Screen saver lock must be activated when devices are left unattended (Staff Only)	
8.	Enforced Password policies that include (Staff Only): • Maximum 90 day enforced password change • Minimum Password length 8 Characters • Complexity requirements with a minimum of uppercase/lowercase characters and base digits (0-9).	
9.	Appropriate access controls are in place on shared drives	
10.	Employee/student related information is not stored within shared drives that have open access to all users	
11.	Appropriate quotas are allocated to student and staff accounts (enforcing staff/students to clean up work areas)	
12.	All software must have an appropriate license	
13.	All emails that contain data related to pupils or staff that are sent outside the academy must be encrypted (128 bit minimum)	
14.	All official external email must carry the official academy disclaimer (see section 6.1 Email Policy)	
15.	Up to date virus protection software must be installed on all academy devices	
16.	All staff accessing academy emails on Smartphones **must setup a pin code security**	
17.	Images of students should not be taken/stored on any personal mobile device. Images taken using academy mobile devices must not be removed from academy premises without authorisation from the Principal	
18.	Any removable media device used for confidential data must be encrypted **(preferred level FIPS 140-2 Level 3 certification)**	
19.	All academy devices used by staff off site must be encrypted if they are used to store academy data	
20.	All server/hub rooms must be kept locked with a limited number of personnel access.	
21.	A backup and disaster recovery solution is in place at the academy	
22.	All backup tapes/drives if stored onsite must be kept in a secure location (preferably in a fire proof safe)	
23.	Outside contractors must be supervised at all times when working in sensitive areas such as Hub/server rooms	
24.	MIS system access is monitored and recorded (appropriate rights are assigned)	
25.	Single sign on is not applied to the MIS system	
26.	The academy has a clear, progressive e-safety education programme for its students/Staff/governors/parents	
27.	Staff are fully aware of the social media policy that is in place within NET	
28.	E-Safety information must be accessible through the academies website with a direct link to the CEOP website	
29.	All redundant 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	

PRIVACY NOTICE (STAFF)
Kirk Balk Academy

Privacy Notice - Data Protection Act 1998
Northern Education Trust is the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the Trust about those employed or otherwise engaged to work in our academies. This is to assist in the smooth running of each academy and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body and the School Support Staff Negotiating Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the Trust without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:

- The Department for Education (DfE)
- The LA with administrative responsibilities for the area in which the academy is situated

If you want to see a copy of the information about you that the Trust hold and/or share, please contact Andy Thom, Clerk to the Board at andy.thom@northerneducationtrust.org

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- https://www.barnsley.gov.uk/services/information-and-privacy/your-privacy/
- http://www.education.gov.uk/schools/adminandfinance/schooladmin/a0077963/what-the-department-does-with-school-workforce-data

If you are unable to access these websites, please contact the LA or DfE as follows:

- Data Protection Officer,
  Barnsley Council
  PO Box 634
  Barnsley
  S70 9GG
  Tel: 01226 743555

- Public Communications Unit
  Department for Education
  Sanctuary Buildings, Great Smith Street
  London
  SW1P 3BT
  Website: www.education.gov.uk
  Email: info@education.gsi.gov.uk
  Telephone: 0370 000 2288.

PRIVACY NOTICE (STUDENTS)
Kirk Balk Academy

Privacy Notice - Data Protection Act 1998

Northern Education Trust is a data controller for the purposes of the Data Protection Act. We collect information about your child and may receive information about your child from the previous school and the Learning Records Service. We hold this personal data and use it to:

- Support teaching and learning
- Monitor and report on progress
- Provide appropriate pastoral care
- Assess how well the school is doing

This information includes contact details, national curriculum assessment results, attendance information and personal characteristics such as ethnic group, any special educational needs and relevant medical information. If your child is enrolling for post 14 qualifications, we will be provided with a unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications your child has undertaken.

Biometrics
Where our academies use a recognition system using biometrics; which allows us to make the best use of efficient systems such as cashless catering, library software, and print & copy control, the Trust also:

- Ensures that the pupils 'biometric data is treated with appropriate care and complies with the data protection principles as set out in the Data Protection Act 1998
- Ensures that where data is to be used as part of an automated biometric recognition system that it complies with the additional requirement in sections 26 to 28 of the Protection of Freedoms Act 2012
- Ensures that each parent/child is informed about the use of the biometric systems at the academy
- Ensure that at least one parent has given written consent before data is taken to be used with any biometric system.
- Provides reasonable alternatives of accessing services for those pupils who have opted out of using the system.
- Ensures that all biometric data that is stored is encrypted
- Ensure that all biometric data is erased when a pupil leaves the academy
- Has systems in place that allows parents to withdraw their consent at any time (must be in writing in the form of a letter or email)

In addition
Once your child is aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your child's and your name(s) and address, and any further information relevant to the support services' role. However, if your child is over 16, you (or your child) can ask that no information beyond names, address and your date of birth be passed to the support service. This right transfers to your child on their 16th birthday. Please inform Mrs M Pedler if you wish to opt-out of this arrangement. For more information about young peoples' services, please go to the Directgov Young People page at:

www.direct.gov.uk/en/YoungPeople/index.htm

or the LA website:
https://www.barnsley.gov.uk/ *]*

We will not give information about your child to anyone outside the academy without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that the Trust hold and/or share, please contact Mrs M Pedler

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

https://www.barnsley.gov.uk/services/information-and-privacy/your-privacy/

http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Data Protection Officer,
Barnsley Council
PO Box 634
Barnsley
S70 9GG
Tel: 01226 743555

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk
Email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

E-safety useful links & resources

Parent Info - Expert information to help children and young people stay safe online http://parentinfo.org

CEOP (Child Exploitation and Online Protection Centre) - www.ceop.police.uk

Think U Know – Provides the latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. If you look after young people there are resources you can use in the classroom or at home. There's also a place which anyone can use to report if they feel uncomfortable or worried about someone they are chatting to online. - www.thinkuknow.co.uk

Childline – Advice and support for children and young people - www.childline.org.uk

Childnet International - working with others to help make the internet a great and safe place for children - www.childnet.com

Internet Watch Foundation (IWF) - UK Hotline for reporting criminal online content - www.iwf.org.uk

UK Safer Internet Centre – Summarised research on e-safety – www.saferinternet.org.uk/research ; Education packs - www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

Digital Parenting Magazine – Online e-safety resources for parents - www.vodafone.com/content/parents.html

Digital Me – Safe - Safe is a programme of practical activities that develop young people's skills, self-confidence and safety awareness when using social networking sites. - www.digitalme.co.uk/safe

Information Commissioner's Office (ICO) - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. - https://ico.org.uk

UK Council for Child Internet Safety (UKCCIS) - www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Government Guidance – Radicalisation using social media - Guide for schools on how terrorist groups such as ISIL use social media to encourage travel to Syria and Iraq. www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Better Internet for Kids - www.betterinternetforkids.eu

Anti-Bullying Network - Cyber-Bullying information for teachers and other professionals who work with young people – www.antibullying.net/cyberbullying1.htm

Cyberbullying Research Centre - http://cyberbullying.org/

Know the Net - www.knowthenet.org.uk/knowledge-centre/child-safety

Family Online Safety Institute - www.fosi.org

Facebook Advice to Parents - www.facebook.com/help/search/?query=parents

Get Safe Online - www.getsafeonline.org/

NET E-Safety Posters (see below)

E-Safety

CLICK CEOP
Internet Safety

www.ceop.police.uk

With the increase in the popularity and use of the internet, it has quickly become an essential part of daily life. The internet is used for emailing, playing games, file searching, social networking and much more. While these are beneficial and exciting ways of keeping in touch with friends and family, there are always risks involved

Tips for staying Safe

- Never give out any personal details (full name, home or school address, telephone number, email) to anyone you meet whilst on the internet, always use a nickname.
- Never agree to meet up with someone you don't already know.
- Never reply to any spam or junk emails you receive
- Don't accept any friend requests, reply to emails or messages from people you don't already know
- Don't post or send offensive messages, emails or pictures
- When downloading files make sure they are from a trusted source and only do so with permission (parent/guardian)
- Don't share your username or passwords
- Stay away from inappropriate websites
- Try to have your online conversations in public, people are less likely to hassle you if other people can see them doing it.
- If someone makes you feel uncomfortable or worried then report it immediately to an adult (Head of School/Parent/Guardian)

Be aware that

- People might not always be who they say they are
- Spam or junk emails may hold viruses that could harm your computer
- What you put online is widely available for others to see

Northern Education Trust

Useful Information

Childnet:
www.childnet.com

UK Safer Internet Centre:
www.saferinternet.org.uk

Digizen:
www.digizen.org

KidSMART:
www.kidsmart.org.uk

Chatdanger:
www.chatdanger.com

Facebook Family Safety Centre:
www.facebook.com/safety

Google+ Safety Centre:
www.google.com/+/safety

Remember report any abuse to
(Head of School/Parent/Guardian)

CLICK CEOP Internet Safety

To report actual or attempted abuse online click on this icon on the academy website or go to www.ceop.police.uk

Northern Education Trust

USEFUL INFORMATION

Childnet International — www.childnet.com

UK Safer Internet Centre — www.saferinternet.org.uk

KidSMART — www.kidsmart.org.uk

digizen.org — www.digizen.org

www.google.com/+/safety

www.facebook.com/safety

CLICK CEOP Internet Safety

To report a case of actual or attempted abuse online, click on this icon on the academy website or go to **www.ceop.police.uk**

TIPS FOR STAYING SAFE:

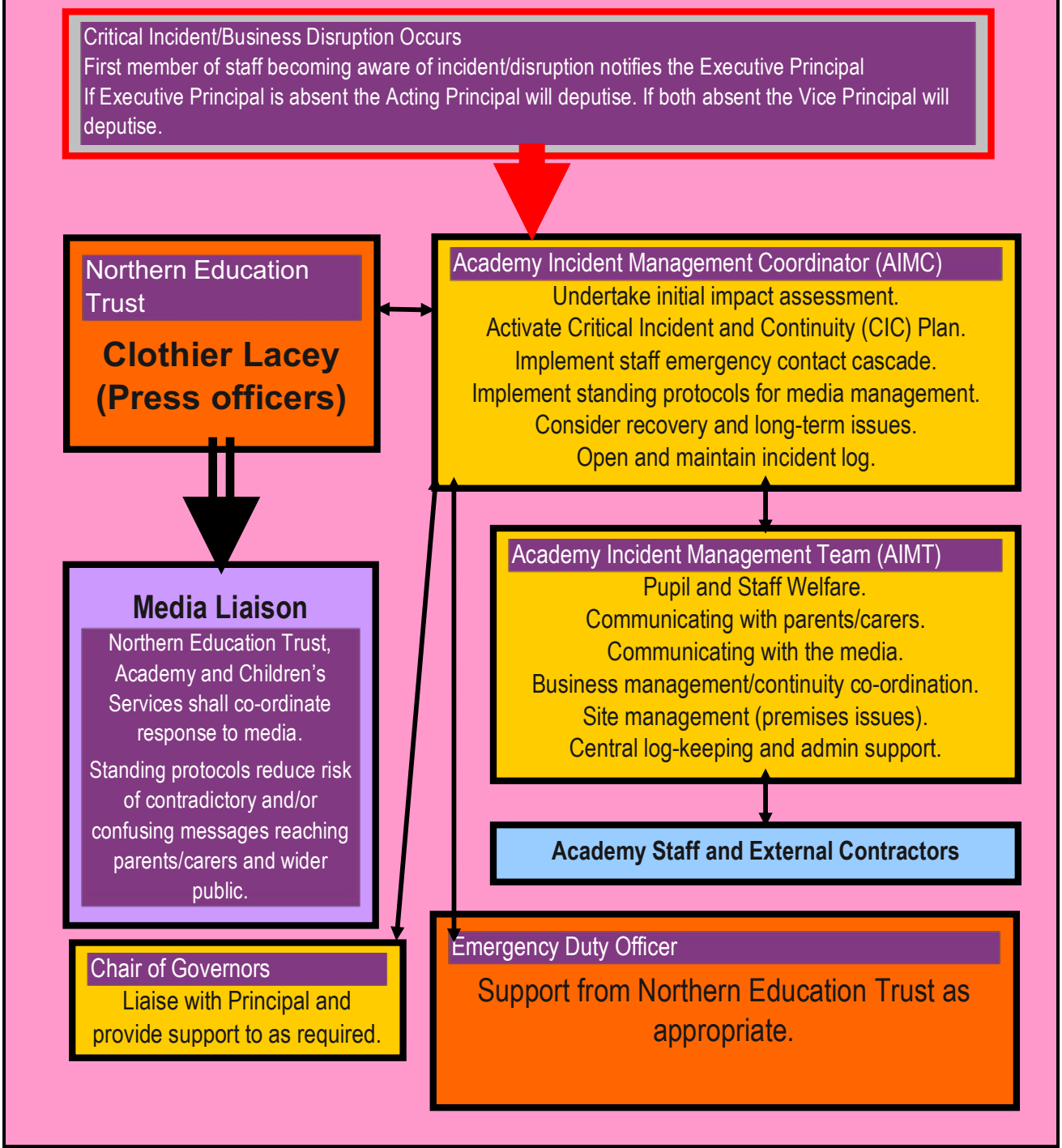
- **Never** give out any personal details (such as full name, home or school address, telephone number, email) to anyone you meet whilst on the internet. Instead, always use a nickname.
- **Never** agree to meet up with somebody you don't already know.
- **Don't** accept any friend requests or reply to emails or messages from people you don't already know.
- **Don't** send or post offensive messages, emails or pictures.
- When downloading files, make sure they are from a **trusted source** and only do so with the permission of your parent or carer.
- **Don't** share your user name or passwords.
- Stay well away from **inappropriate websites**.
- Try to have **online conversations in public**. People are less likely to hassle you if other people can see them doing it.
- If someone makes you feel uncomfortable or worried then **report it immediately** to an adult (teacher, parent, carer)

BE AWARE THAT:

- People may not always be who they say they are.
- Spam or junk emails may hold viruses that could harm your computer.
- What you put online is then widely available for others to see.

Incident Response Flowchart and Log (Refer to Critical Incident and Continuity Plan)

Responding to a Critical Incident or Business Disruption [Action Card ER/02]



Key Operating Priorities

Operating priorities that shall be addressed at all times during implementation of this plan are:

- Safety of Students, staff and visitors.
- Maintaining learning and extended services.
- Minimising financial loss.

Log of Events, Decisions and Actions [Action Card IM/11: Part 1 of 2]

Name		**Sheet Number**	
Role			
Incident		**Date**	
Time	**Log Details**		

'Time' should be recorded in the 24 hour format (for example 1.30pm shown as 13.30).

'Events' will include all in-coming/out-going communication and key meetings.

'Decisions' will include the sanctioning of actions and reasons where action will not be taken. Any expenditure incurred should be recorded.

'Actions' will include confirmation that sanctioned actions have been completed.

Continue on Part 2 (as required)

Legal Framework

Protection of Children Act 1978 It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Racial and Religious Hatred Act 2006 This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003 Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003 It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison. The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).
Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Academies should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127) Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998 protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

The Computer Misuse Act 1990 (sections 1 - 3) This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1) This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988 Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trade Marks Act 1994 This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Public Order Act 1986 (sections 17 — 29) This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964 Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997 A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000 The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Regulation of Investigatory Powers Act 2000 It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to: Ascertain whether the communication is business or personal; Protect or support help line staff. The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008 Section 63 offence to possess "extreme pornographic image" 63 (6) must be "grossly offensive, disgusting or otherwise obscene" 63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006 Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/ Bullying:
Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

Telecommunications Act 1984 It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994 This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998 This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.