Castle View Academy
The best in everyone™

Technology Policy

Responsibility: IT Manager
Review Schedule: Annual
Reviewed: September 2025
Next Review: September 2026

Contents

Scope

This policy applies to all members of the Academy community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of the Academy.

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 cyber-bullying, 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 2011 Education Act 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 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. Sanctions employed should align with the institution's wider behaviour and bullying policies.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the Academy with regards to the use of technology.

Governors

Governors are responsible for ensuring that an Academy complies with its legal obligations. Governors are responsible for the approval of the Technology Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Governor with responsibility for Safeguarding and Child Protection has also taken on the role of E-Safety. The role of the E-Safety
Governor will include:

- regular meetings with the Academy's E-Safety Officer
- regular monitoring of e-safety incident logs
- reporting to relevant Governors meeting

Principal and Senior Leaders

The Principal has a duty of care for ensuring the safety (including e-safety) of members of the Academy community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Officer.

The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant United Learning HR disciplinary procedures).

The Principal/Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer

The E-Safety Officer:

- leads the e-safety committee;
- takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy's Technology Policy and other documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with United Learning, Local Authority and relevant bodies;
- liaises with Academy technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs;
- attends relevant committee of Governors;
- reports regularly to Senior Leadership Team.

Network Manager

The Network Manager is responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the Academy meets required e-safety technical requirements and any other relevant body Technology Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced Password Protection Policy, in which passwords are regularly changed.
- that they keep up to date with e-safety technical information to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network and all associated access is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Officer for investigation/action/sanction.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of the safe use of technology and e-safety matters and of the current Academy Technology Policy and practices.
- they have read, understood, and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the E-Safety Officer for investigation/action/sanction.
- all digital communications with students/parents/carers are on a professional level.

- e-safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the Technology and Acceptable Use Policies.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead (DSL)

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the Academy community, with responsibility for issues regarding e-safety and the monitoring of the Technology Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Group (or other relevant group) will assist the E-Safety Officer with:

- the production/review/monitoring of the Academy Technology Policy/documents
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and the students about the e-safety provision

Students

Students must:

- use the Academy digital technology systems in accordance with the Student Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.

- understand the importance of adopting good e-safety practice when using digital technologies out of Academy and realise that the Academy's Technology Policy covers their actions out of Academy, if related to their membership of the Academy.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The Academy will take every opportunity to help parents understand these issues through a variety of methods. Parents and carers will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events
- parents' sections of the website and on-line student records
- their children's personal devices in the Academy (where this is allowed)

Breaches of the Policy

By Students

Any breach of this policy may lead to disciplinary action being taken against the student/s involved in line with the Academy's Behaviour Policy.

By Staff

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with United Learning's Disciplinary Policy. A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the Academy or United Learning or any illegal acts or acts that render the Academy or United Learning liable to third parties will result in disciplinary action appropriate to the severity of the breach.

By Contracted Providers of Services

Contracted providers of services to the Academy/United Learning must inform the Academy/United Learning immediately of any breaches of this policy by their staff so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the Academy/United Learning. Any action against breaches should be according to contractors' internal disciplinary procedures.

E-Safety Policy

Introduction

The E-Safety Policy is a key element of the Technology Policy as it is about the safe and responsible and ethical use of online technologies. It covers accessing online resources through computers, tablets, smart phones and any other internet enabled device safely and effectively. In conjunction with the Social Media policy, it includes new social media tools and other emerging trends. It should cover a range of issues and not condemn the use of tools but rather address how to use them safely. This should include how to comment appropriately in many different forums, including social media and not being just a bystander. An essential part of this is how to report concerns, online and offline.

The policy will outline who will deliver the training, in which subject area and to which parts of the Academy community. It also references how the effectiveness of the processes is monitored.

Key Personnel

Mr Matt Gill – Interim Principal
Mrs Sarah Pennington-Chick – Vice Principal/E-Safety Officer
Mr Chris Bonner – Network Manager

Areas of Risk

Child Protection	Children are exploited by sex offenders Children upload inappropriate content online Children publish personal information which identifies them either overtly or covertly (location metadata in images or messages) Staff do not understand the technology and under (or over) estimate the risk
Staff Protection	Staff post comments or images which compromise their professional integrity Staff's lack of understanding of new online tools put them at risk
OFSTED Inspection	Lack of understanding of the E-Safety Policy by staff, students or governors can prevent a school from achieving an excellent or outstanding inspection judgement.

Scope

This E-Safety Policy should be read in conjunction with other policies with the over-arching Technologies Policy but with particular reference to the Mobile Devices Policy, Social Media Policy and Internet Filtering Policy

Policy Statements

Communicating with children electronically

Any electronic contact between a staff member and a student should be via the staff Academy email address only and should be formal in nature.

Education: Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Academy's e-safety provision. Children and young people need the help and support of the Academy to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of PHSE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT staff can temporarily remove those sites from the filtered list for the period of study.

Education: Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web sites
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

- Reference to relevant websites/publications e.g.: www.swgfl.org.uk or www.saferinternet.org.uk/ or http://www.childnet.com/parents-and-carers

Education & Training: Staff/Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy E-Safety Policy and Acceptable Use Agreements.
- The E-Safety Officer (or other nominated person) will receive regular updates through attendance at external training events (e.g., from United Learning/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- The E-Safety Coordinator/Officer (or other nominated person) will provide advice/guidance/training to individuals as required.

Training: Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation
- Participation in Academy training/information sessions for staff or parents

E-safety Information

- **Internal resources**
  The school website and through core ICT lessons
- **External resources**
  The school website and associated links

Reporting Procedures

- **Internal reporting**
  This should be reported using the internal 'Harm' forms. For staff, any concerns should be dealt with using the school Safeguarding and Whistleblowing Policies. These are then reported to the Governing Body.
- **Monitoring Reports**
  Reporting will be to the Governing Body on a termly basis as part of the Safeguarding and Child Protection Report.
- **External Reporting**

The school website contains a significant number of links to other agencies that provide advice and guidance if and when required.

Monitoring Success

The Academy will monitor the success of policies via the number of incidents reported to governors on a termly basis. The effectiveness of the policies will be reviewed every two years.

Mobile and Other Electronic Devices Policy

Introduction

The majority of students and staff, for security and practical reasons, feel the need to carry a mobile phone, and for these reasons their use is allowed in Academy. However, as we are a working community, we need to have regulations governing the use of Wi-Fi and 3G/4G enabled devices so that incoming communications do not interrupt lessons and so that students do not use them unnecessarily and disrupt the effective operation of the Academy.

This Policy applies to 'standard' mobile phones as well as smart phones and other 3G/4G/5G and WiFi enabled devices such as iPads, iPods, tablets and laptops. Use of mobile devices by members of staff and students is regulated, in accordance with Group policy and recognised professional standards of acceptable practice.

This policy should be read in conjunction with the Academy's Acceptable Usage Policy for Technologies.

The Academy accepts that staff and students are permitted to bring such devices to the Academy, but their use is restricted as detailed in this policy.

This policy applies to all members of the Academy community.

This policy is reviewed at least annually by the Academy senior management, who will report to the Local Governing Body on its implementation.

The policy should be made available on the Academy's website and in hard copy form from Reception. It should be read in conjunction with:

- Behaviour and Discipline Policy
- Anti-Bullying Policy

The Academy is committed to ensuring that the implementation of this policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the Academy's own Equal Opportunities Policy.

Area of Risk

Child Protection:	Pictures of children on the at-risk register become associated with the school through linked social media platforms
Bullying:	Use of mobile technology can make bullying more pervasive and difficult to monitor
Staff Protection:	Content recorded in lessons, whether overtly or covertly, on mobile devices may cause distress to staff, especially when uploaded to social platforms.

Procedures

A commonsense approach should be followed regarding the use of 3G and Wi-Fi enabled mobile devices. Teachers should always have the ability to override rules against mobile device use, where common sense prevails, although the following guidelines should be used:

Policy Statements

Times and locations where mobile devices may be permitted

- When directed by a teacher and within the context of an academic lesson, students may be given permission to use social media.
- When directed by a teacher and within the context of an academic lesson, students may be given permission to video each other or themselves on their own devices.
- Taking photos on Academy trips - if students use their own devices on an informal basis to take photographs of other students whilst on Academy trips, they must give due consideration to the appropriateness of uploading any photographs or video to social media sites.
- Taking photographs of academic work. There are times when students will want (or need) to photograph different stages of a project, practical task or experiment. In all cases, students should seek authorisation from their teacher before using cameras to record their work.
- Under direction from a member of staff, students may use either Academy owned cameras or their own personal mobile device to make an appropriate record of their academic work. Staff may withdraw authorisation at any time and students should be mindful of the responsibility given in allowing use of personal devices. Any images or sections of video, which are found to contain images of students, should be deleted at the earliest opportunity.
- A student may be given authorisation to video or record specific elements of a lesson, at the sole discretion of the teacher of the lesson. For example: Record explanations of key theories for listening to again later, videoing a science experiment to upload to VLE.
- No content recorded by a student on a personal device should be uploaded to a social media, video sharing (such as YouTube) or photograph sharing site (such as Flickr), without the permission of those being filmed, including members of staff. Doing so could result in disciplinary action.

Times and locations where mobile device use is not permitted

- 3G/4G or WiFi enabled devices of any description, including mobile phones, iPods or iPads, must never be taken into public examinations by students or staff.
- Mobile devices should be switched off or muted and in airline mode during lessons, unless directed otherwise by the member of staff in charge.
- Students should not be posting updates to social media platforms during the Academy day unless specifically directed to do so by a member of staff for educational purposes.
- Students should not post information about their specific location or current activity to social media platforms while on an Academy trip. In doing so students could affect their personal safety or that of their peers.
- Students should not contact their parents directly when unwell or unhappy at the Academy, via either phone, social media or electronic methods, to arrange to be collected. The student should report to the Academy office who will contact their parents, if appropriate.

- Parents should telephone the Academy office in the event of an emergency, and a message will be passed on in the usual way.
- In line with the Academy policy on use of photographs taken in the Academy, students are not allowed to use their mobile devices or cameras to take photos or videos of other students for any Academy purpose. It is not, for example, permissible for students to use their own devices to take videos of e.g., auditions for an Academy event, or a classroom activity.
- If students need to be filmed for such purposes, filming must be sanctioned by the member of staff concerned; agreed to by the student(s) concerned; and be on Academy devices only.
- Parents must agree to the Academy using its own devices to film students on occasion for internal use when their child joins the Academy.
- Under no circumstances should covert recording of lessons take place or recording take place outside of the specific parameters laid out by the teacher when authorisation is given. Doing so could result in disciplinary action
- Uploading inappropriate photos or videos could result in disciplinary action, as outlined in the Student Acceptable Use of Technology Policy.

Sanctions for Misuse of Mobile Devices

Should mobile phones be used inappropriately, the consequences will follow the Academy's Behaviour Policy. This may include confiscation until the end of the lesson/day or longer for serious issues. For persistent offenders, phones will only be returned to parents. The Academy will also apply appropriate sanctions to any student or member of staff who uses their mobile phone, or other device, for bullying, intimidation, or for keeping, or disseminating inappropriate text or images.

Security of Mobile Phones and Other Electronic Devices

Students and staff are advised to have their phones/iPods/iPads security marked.

The Academy does not accept responsibility for mobile phones or other electronic communication devices or entertainment systems. Parents (and staff) should be informed that mobile phones and other such devices are not covered by the organisation's insurance policy. Staff should be advised to keep valuables on them at all times or secure them appropriately should this not be possible.

Cyber Bullying

Instances of cyber bullying will be punishable in accordance with the Academy's Anti-Bullying Policy and may even result in exclusion or expulsion (or in disciplinary action, in the case of staff). In some circumstances students may, for example, be asked to leave their mobile devices with the Principal of Year for a specified period of time during the Academy day.

Dealing with Inappropriate Content on Mobile Devices

If a teacher suspects or is informed that a student has inappropriate content on their mobile device then the teacher will confiscate the device. A Vice Principal will investigate the matter and report to the Principal. During their investigations, if the student is formally interviewed,

this will be with another member of staff present. A member of staff may investigate content on the mobile device as part of an investigation and in line with the Academy's Electronic Devices – Search and Deletion Policy. The student's parents may also be invited to attend the interview. It may be appropriate for the young person to be excluded whilst an investigation takes place.

If it is discovered that the student's mobile phone (or other electronic device) contains inappropriate images of a child or young person (under the age of 18), the Principal will be informed and the PCSO or Police liaison officer. The mobile device will remain in the possession of the Principal until advice from the police has been acted upon. This may include asking all students in possession of the image to delete it or if the image has been forwarded outside the Academy's control, contact will be made to request that third parties follow the same steps. If the image has been uploaded to any website or social networking site, contact will be made in an attempt to have it removed. The parents of all of the students involved will be notified of the situation to ensure all content on devices in the homes of the students are removed. In-house counselling will be offered to those concerned if appropriate.

In the case of staff, any instances of inappropriate images of children or young people must be reported immediately to the Principal, or in his absence to the Vice Principal (Student Entitlement).

Use of mobile devices: guidelines for staff use (photographs and videos)

The Academy recognises that it is not always practical for teachers to borrow the Academy camera for events and trips and that photographs of such activities form an integral part of key publications such as the Newsletter. Staff are therefore allowed to use their own devices to take photographs of children if it is not practical to borrow the Academy camera, having received authorisation from their line manager and fully understanding the implications of devices which are synchronised to online storage (see online storage guidance).

Staff must under no circumstances ever use any photographs of students for anything other than strictly professional purposes. They must never upload photographs or videos of any students onto the internet or social media sites. The only exception is to use photographs of students, where parents have given consent, on the Academy's own website or other Academy managed social media platforms.

If staff are using social media websites such as Facebook or Twitter to e.g., set up subject pages, they should not upload any photographs of students themselves, unless they are following strict Academy guidelines and are aware of which students should not be photographed.

After taking photographs of students with their own devices, staff should not store these for any longer than necessary, and once copied onto the Academy network should be deleted from all personal devices, including online storage.

Before printing any photographs of students in any external publication (e.g., local or national newspapers), parents must give permission for the student's photograph and/or name to be used.

Mobile Device Guidelines for Students

- All devices are brought into Academy at the student's own risk and the responsibility for their safekeeping lies with the student. The Academy will take no liability for loss or damage.
- Academy is a place of work; students' mobile phones/devices must be switched off (or in silent mode) at all times whilst on Academy premises, unless specifically authorised by a member of staff. Mobile phones should not be seen during the hours of 08:30-15:00 without the permission of a teacher.
- If the use of a device is permitted or directed in a lesson (e.g. as a calculator, camera or voice recorder) it will be under explicit staff supervision, and permission can be withdrawn at any time.
- Any student found using a device on Academy premises without staff permission, should ordinarily expect to have their device confiscated for the rest of the day and should collect it as instructed.
- If a student needs to contact home in an emergency, they must speak with a member of staff who will deal with the matter. Students should not contact home in the case of illness; this should only be done by a member of staff.
- If parents need to contact students in an emergency, they should contact the Academy reception and a message will be taken to the student.
- The accessing, or updating, of social media platforms is not permitted unless it is part of a structured educational activity.
- Students should be aware that under no circumstances should they enter an examination venue with a device, even if it is switched off. To do so may lead to disqualification from that examination and potentially other examinations.
- Students should note that the use of all devices on Academy premises is subject to the Academy's Technology Acceptable Usage policy.

Mobile Device Guidelines for Staff

- Staff personal mobile digital devices should be switched off (or in silent mode) during lessons, or at times where they are responsible for the supervision of students.
- Staff should not use a personal mobile digital device, or similar, during lessons (or when supervising students) to receive or send personal calls, texts or post content to personal social media platforms.
- If a member of staff feels that it is necessary to be available to receive a personal call or text on a personal mobile device during a lesson, for which there may be exceptional circumstances, they should explain this to their line manager beforehand.
- Staff should not use a personal mobile digital device, or similar, during lessons (or when supervising students) to access online resources, emails, apps or similar, unless it is considered that the outcome is essential to student learning and cannot be sourced through the Academy network (in which case, students should be made aware that the mobile device has been used for this educational purpose).

- Staff must not photograph or video students with a personal (mobile digital) device. If it is necessary to regularly take images of students, then an Academy owned device should be provided.
- Staff should endeavour to make any personal calls on their own mobile telephone, or similar, in a discreet fashion and away from any student area, for example in the Staff Room or in an office, behind closed doors.
- Staff should not give out their personal mobile phone numbers, or other communication contact information, to students.
- Inappropriate use of mobile devices is a serious offence; cases of misuse could lead to disciplinary action being taken against the individual concerned.

Summary Points for Classroom Display

- The Academy is a place of work; students' mobile phones/devices must be switched off (or in silent mode) at all times whilst on Academy premises, unless specifically authorised by a member of staff. Mobile phones should not be seen between the hours of 08:30-15:00 without the permission of a teacher.
- If you need to contact home in an emergency, ask permission from a member of staff first.
- If you are unwell, the Academy will contact home on your behalf, if needed.
- You are responsible for the safekeeping of your device.
- If you are found using your device, without staff permission, you should expect to receive a detention and your device will be confiscated.

Electronic Devices Policy - Searching & Deletion

The changing face of information technologies and ever-increasing student/staff use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to academies by statute to search students in order to maintain discipline and ensure safety. Academies are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the Academy will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the Academy with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the Academy rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the Academy rules are determined and publicised by the Principal (section 89 Education and Inspections Act 1996).

An item banned by the Academy rules may only be searched for under these new powers if it has been identified in the Academy rules as an item that can be searched for. It is therefore important that there is an Academy policy which sets out clearly and unambiguously the items which:

- are banned under the Academy rules; and
- are banned AND can be searched for by authorised Academy staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the Academy rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Principal must publicise the Academy's Behaviour Policy, in writing, to staff, parents/carers and students at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).
Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The Academy Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989

- Human Rights Act 1998
- Computer Misuse Act 1990

Responsibilities

The Principal is responsible for ensuring that the Academy's policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Principal will need to authorise those staff who are allowed to carry out searches.
The Principal has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: ALT, Principals of Year, Key Stage Managers.

The Principal may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training/Awareness

Members of staff should be made aware of the Academy's policy on "Electronic devices – Searching and Deletion":

- at induction
- at regular updating sessions on the Academy's E-Safety Policy

Members of staff authorised by the Principal to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search

Academy staff can search a student for any item if the student agrees.
The Principal and staff authorised by the person holding this position have a statutory power to search students or their possessions, without consent, where they have reasonable grounds for suspecting that the student may have a prohibited item.

Prohibited items are:

- knives or weapons
- alcohol
- illegal drugs
- stolen items
- Tobacco and cigarette papers
- fireworks
- pornographic images
- any article that the member of staff reasonably suspects has been, or is likely to be, used to commit an offence, or

- to cause personal injury to, or damage to the property of, any person (including the student).

This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.
Students are allowed to bring mobile phones or other personal electronic devices to Academy and use them only within the rules laid down by the Academy in the Mobile Devices Policy.

If students breach these rules:

The sanctions for breaking these rules can be found in the Mobile Devices Policy.

Authorised staff have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the Academy rules.

Searching with consent: Authorised staff may search with the student's consent for any item.

Searching without consent: Authorised staff may only search without the student's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the Academy rules as an item which is banned and may be searched for.

In carrying out the search

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e., an item banned by the Academy's rules, and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g., an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the student being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search

The person conducting the search may not require the student to remove any clothing other than outer clothing.
Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.
A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g., a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the Academy rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the Academy open to legal challenge.
If a member of staff is shown an inappropriate material on an electronic device, they must act to confiscate the device in an appropriate way. THE STAFF MEMBER MUST NOT SEND THE MATERIAL OR PRINT OR COPY THE MATERIAL IN ANYWAY AS THIS IS DEEMED TO BE 'DISTRIBUTING' AND IS A CRIMINAL OFFENCE.

Examples of inappropriate materials are listed below;

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If a child states that the material is inappropriate then the staff member should not seek to view it but report this to the safeguarding team who will use standard procedures and appropriate agencies to support the child.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any

data or files, if they think there is a good reason to do so (unless the data or files are criminal in their nature - this should be reported to the safeguarding team). Examples of data that can be deleted are pictures taken of an appropriate nature without the persons consent.

Care of Confiscated Devices

Academy staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices.

Social Media Policy

This policy statement is intended to serve as guidance for United Learning academies which are responsible for developing and implementing their own policy, tailored to their specific context. It is not anticipated that any Academy will adopt this document without amendment.

The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on Twitter/X and maintaining pages on internet encyclopedias such as Wikipedia.

While recognising the benefits of these media as new opportunities for communication, this policy sets out the principles that United Learning staff and contractors are expected to follow when using social media.

It is crucial that students, parents and the public at large have confidence in the Academy's decisions and services.

The principles set out in this policy statement are designed to ensure that staff members use social media responsibly so that confidentiality of students and other staff and the reputation of the Academy and United Learning are safeguarded.

This policy statement also aims to help staff use social media with minimal professional risk. Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Key Personnel

The Principal will oversee the implementation of this policy supported by the E-safety Officer, School Manager and Network Manager.

Scope

This policy covers personal use of social media as well as the use of social media for official United Learning/Academy purposes, including sites hosted and maintained on behalf of either.

This policy applies to personal web presences such as social networking sites (for example Facebook) blogs and microblogs (such as Twitter), chatrooms, forums, podcasts, open access online encyclopedias (such as Wikipedia), social bookmarking sites (such as del.icio.us) and content sharing sites (such as Flickr and YouTube). The internet is a fast-moving technology, and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Legal Framework

United Learning is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of United Learning are bound by a legal duty of confidence and other laws to protect the confidential information

they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

Staff should also be aware of the guidance and sanctions contained within the United Learning Disciplinary Policy.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g., student and employee records protected by the Data Protection Act 1998 (see Data Protection Policy)
- Information divulged in the expectation of confidentiality
- Academy or United Learning business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.
- Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:
- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

The Academy and United Learning could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render the Academy and United Learning liable to the injured party.

Professional Use of Social Media

Many academies maintain presences on various social media sites as they provide very effective additional channels of communication with parents/carers, students and the wider community.

For example, Twitter/X is used to collate and publicise a stream of positive messages about the multitude of activities that go on at United Learning's academies every day. Some staff have chosen to play a part in this use of social media for professional purposes, often to highlight successes and to encourage participation in their area of work.

This is not without risk, however and staff members should be aware that:

- services such as Twitter/X are in the public domain and are regularly used by journalists, students, parents and employers.
- submissions can take on a life of their own once sent by users, who should not rely on being able to delete them.
- The Academy and United Learning may re-tweet the submissions of staff members to their wider following.
- Students or parents may retweet comments and pictures which directly relate to them, their family or their friends.
- The ability to post anonymous comments to social media platforms, such as Twitter, may result in offensive or upsetting comments being directed at the Academy or staff.

Policy statements

Staff members must not upload video content to hosting services (such as YouTube) without sign off from the Vice Principal (DSL) or Principal. This is for reasons of safeguarding and for maintaining the reputation of the Academy and United Learning. Likewise, staff members must not make use of any social media service with students apart from the Academy's Learning Platform or the BiE Cloud, unless a pedagogical business case and associated risk assessment is agreed.

Staff members should maintain a professional persona through any use of social media for work purposes. Usernames should be formal (e.g. @MrSmith_AcademyName) or anonymised (e.g. @PE_AcademyName). The latter option also distances the user from their real-life identify and makes online bullying less likely.

All professional submissions to social media sites must show the Academy and/or United Learning in a positive light and should be written without ambiguity or any rhetorical device (such as sarcasm) which might be misinterpreted. It is surprisingly easy for even the gentlest of humour to be read differently than intended when parsed through abbreviated media such as Twitter.

Staff members must not enter into dialogue using social media such as Twitter, which the Academy and United Learning are using purely as a one-way channel for distributing news. Any attempt by other users to interact with staff members via such services should be reported to the School Manager/Principal/appropriate delegated leader for advice and resolution. The simplest option is usually to take such issues offline. Even the simple act of responding to a student's tweeted question confirms that the student attends the Academy, links to their wider digital identity and photographs of them and does so in a purposefully public forum.

Staff members should exercise professional judgement when using social media. If new to social media it is good practice to ask a senior colleague's opinion before posting an update to a social media service. If in doubt over the appropriateness of a submission, the best option is not to make it. Appropriate disciplinary action will be taken should a member of staff make a submission which brings the Academy or United Learning into disrepute.

Any images submitted to a social media site should be chosen carefully and should show the Academy positively.

Images of students must only be uploaded with exceptional caution; no individual or close up images should be used where the student could be identified without parental permission. Likewise, no image which might reasonably be judged to cause embarrassment to the student should be published. 'Over the shoulder' images (where individuals are not recognisable) or group shots of 3 or more students are safest. Staff should seek advice from a senior colleague before publishing images of students wearing PE kit.

Images of individual staff should only be uploaded with their consent and no image which might reasonably be judged to cause embarrassment to the member of staff should be published.

Individual students should not be identifiable through submissions to social media sites, for safeguarding reasons. For example, "Excellent piece of Level 7 work shown here by Tom in Y8" is acceptable, whereas including Tom's surname is not. Any submission that includes an image of a student must not make reference to the student's first, sur- or full name under any circumstances.

Strong password security must be maintained and regularly changed for any social media account, to prevent it from being hi-jacked and misused. Passwords should never be written down. A combination of upper- and lower-case characters should be combined with numerals. The potential for hi-jacked accounts to bring the Academy and United Learning into disrepute is significant and responsibility for account security lies with the staff member who controls it. Staff should be cognisant that such accounts are likely to be targeted by students for precisely this purpose.

Devices used to post content to social media platforms should be password protected to prevent third parties from posting on your behalf.

Fraping (or Facebook raping) is where a third party changes a person's status or posts inappropriate content to a social media platform without their consent or knowledge. The consequences can be long term and damaging.

Personal Use of Social Media

It is reasonable for members of staff to maintain personal web presences in their lives beyond their Academy life. Indeed, in 2012 over 53% of the UK population had a Facebook account.

Academy staff, however, occupy an almost unique professional position due to their work with children and the moral credibility they must maintain. There have been several recent cases where Academy staff have suffered serious professional consequences as a result of poor judgement in the use of social media.

It is worth considering that information (text, images, video) held in web presences:

- is never completely private and can very easily enter the public domain
- can be misinterpreted by audiences it was not originally intended for
- may persist beyond your wishes
- might be copied and used by third parties without your consent.

It is therefore vital that use of social media in staff's lives beyond the Academy be totally separated from their professional identity. However, staff should be aware that even if this separation is strictly adhered to, it remains relatively easy for people (students, journalists, future employers etc.) to connect staff in the Academy with 'private' social media presences.

Policy Statements

Staff members are advised not to identify themselves as employees of the Academy or United Learning in their personal web presences or purport to represent the views of either organisation. This is to prevent information on these sites from being linked with the Academy/United Learning and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services. Do not name the Academy/ United Learning in any biographical detail associated with personal accounts or use their logos or any other identifying information (such as location).

Staff members are advised not to have contact through any personal social medium with any student or member of a students' family, whether from their Academy or any other Academy, unless the students are family members. Even being linked to the children of colleagues/close personal friends carries risks, as many services such as Facebook allow user data to be visible to friends-of-friends.

Staff members should not put themselves in a position where extreme political, religious or philosophical views expressed via social media conflict with those of a public institution such as the Academy. Even if separation of professional and private lives has been maintained, recent case history shows that teachers who express such views have found their position at the Academy to be untenable. This information is now easier to find as it is possible to search Facebook for example, by likes, affiliation and places of employment.

Staff members should not use social media to document or distribute evidence of activities in their private lives that may bring the Academy or United Learning into disrepute. Even if separation of professional and private lives has been maintained, recent case history shows that teachers whose behaviour becomes known through social media have found their position at the Academy to be compromised.

If staff members wish to use the affordances of social media with students, they can only do so through the Academy's Learning Platform or the BiE Cloud. No other service is to be used unless a pedagogical business case and associated risk assessment is agreed by the Principal or an appropriate delegated leader.

Staff members must decline 'friend requests' from students they receive to their personal social media accounts. Instead, if they receive such requests from students who are not family

members, they should discuss these in general terms in class and signpost students to become 'friends' of the official Academy Facebook or Twitter accounts.

On leaving the Academy's/United Learning's service, staff members must not initiate contact with former students by means of personal social media sites whilst that student is under the age of 18.

Staff members must not initiate contact with former students by means of personal social media sites whilst that student is under the age of 18 or in full time secondary or 16 to 19 education. If the former student has family and/or social media friends in their Academy, they should also refrain from initiating contact with former students by means of personal social media sites.

Information that staff members have access to as part of their employment, including personal information about students and their family members, colleagues and other parties must not be discussed on their personal web presence.

Academy email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopedias such as Wikipedia in a personal capacity from work. This is because the source of the edit will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships, or it might be just too embarrassing if too much personal information is known in the workplace.

Staff members must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or the Academy/United Learning.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites to be as strict as possible and to opt out of public listings on social networking sites to protect their own privacy.

Employees should be aware that United Learning has a policy for raising concerns at work and this should be followed should any concerns arise. Using a social networking site to raise any concerns at work will not be considered as appropriate.

Social Networking Standards

Below sets out the standards expected of all United Learning employees when using social networking sites.

DO

- Act responsibly at all times. Even if you do not identify your profession or place of work, please be aware that your conduct online could jeopardise any professional registration and/or your employment.
- Protect your own privacy. Think through what kinds of information you want to share online and with whom you want to share this information. Adjust your privacy settings accordingly. Remember that the more personal information you share online, the more likely it is that something could have a negative impact on your employment. Think about managing your online friends by restricting what kind of information you give them access to.
- Remember everything is public. Even with the highest level of privacy settings, once something is online it can be copied and redistributed, and it is easy to lose control of the information. Work on the assumption that everything you post online will be permanent and will be shared with others.
- Take appropriate action if you are the target of abuse online. If you find yourself the target of bullying or abuse online then you can take action in dealing with this, such as blocking individuals from interacting with you and using the sites' support mechanisms to report inappropriate activity. The Anti-Bullying Policy also sets out support mechanisms to deal with cyber bullying issues.
- Be considerate to your colleagues. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual concerned. Always remove information about a colleague if they ask you to do so.
- Respect the privacy of others. If photographs are taken at a Castle View Academy event then check whether those in attendance expect that any photos may appear on a public social networking site before posting. Remember it may not always be an appropriate way to share information whether work related or not.
- Update any online sources in a transparent manner. In the course of work, employees may find errors or out of date information displayed through online encyclopedias. If updating this information then you must be transparent about who you are and the capacity in which you are doing this. Employees should consult with their line manager before updating or amending any information about Castle View Academy from an online source.
- Remember the benefits. Used responsibly, social networking sites can be accessed to keep up to date with a number of professions and information. Many use Facebook, Twitter and Linkedin to update and communicate with members. Work blogs may also be useful for communication, networking and professional development purposes but must be discussed and agreed with your relevant Manager/Leader.

DO NOT

- Share confidential information online. In line with the Data Protection Act 1998 employees should not share any child/young person/mother/father/carer identifiable information online or any personal information about colleagues. In addition to this, any confidential information about Castle View Academy should not be revealed online.
- Build or pursue relationships with children, young people, mothers and fathers/carers. Even if the child/young person/mother/father/carer is no longer within your care, Castle View Academy and United Learning does not deem this as appropriate behaviour. If you

receive a request from a child/young person/mother/father/carer, many sites allow you to ignore this request without the individual being informed to avoid any offence. If you are concerned about this in any circumstance, please discuss with your Line Manager.

- Use social networking sites to inform professional practice. There are some circumstances/job roles where this may be appropriate however careful consideration and discussions with management should be applied.
- Discuss work related issues online. This takes into account conversations about child/young person/mother/father/carer/colleagues or anything else which may identify Castle View Academy or United Learning online and bring it into potential disrepute. Even if you think these conversations have been anonymised they are very likely to be deemed inappropriate.
- Post pictures of children/young people/their mothers/fathers/carers. Never post pictures online even if they have asked you to do this. Employees should never take pictures of a child/young person/mother/father/carer unless they are relevant. If your mobile phone has a camera then this should not be used in the workplace unless authorised by the Principal.
- Raise concerns about your work. Social networking sites should never be used for raising or escalating concerns at work. If you have concerns then these should be raised through either discussing with your line manager or following the policy/procedure for raising concerns at work.
- Engage in activities online which may bring the Organisation into disrepute. Think through what activities you take part in whilst online and what you do or say that may bring Castle View Academy and United Learning into disrepute. Any reports of this will be reviewed in line with their appropriateness.
- Be abusive to or bully other colleagues. Social networking sites should not be used as a forum for abusive behaviour towards colleagues.
- Post derogatory, defamatory or offensive comments about colleagues, the children/young person/mothers/fathers/carers/your work. Everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate comments.
- All of the above applies to both open and private sections of any social networking site with which employees identify themselves.

Internet Filtering & Monitoring Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

The monitoring of the Internet (or general computer use if key logging software is installed) is a critical element of any filtering policy as it highlights weaknesses in the filtering device, unusual activity by users, interest in extremist material or self-harm. This monitoring is normally surfaced through regular reports to specific staff members who understand student context and the curriculum. These reports should be regularly reviewed (weekly) and appropriate actions documented. Expect significant false positives when initially implemented.

It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering, monitoring and reporting policy to manage the associated risks and to provide preventative measures which are relevant to the situation and context in this school.
Many users are not aware of the flexibility provided by many filtering services at a local level for schools / academies. Where available, schools/academies should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

The Academy needs to consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- Whether to introduce differentiated filtering for different groups / ages of users
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other user monitoring systems (such as key logging applications Impero or Securus) will be used to supplement the filtering system and how these will be used.
- Who will monitor Internet filters and key logging applications, how often these will be monitored, how it will be logged
- Who will receive inappropriate activity reports, actions to be taken and how it will be logged:
    - For students
    - For staff

Key Personnel

The E-Safety Officer and Network Manager will be responsible for reviewing the Internet Filtering & Monitoring Policy. Additional expertise on filtering will also be provided by the IT technician.

The Network Manager and IT technicians will be responsible for reviewing staff/student internet activity and generating reports for review by the DSL/SLT.

Responsibilities

The responsibility for the implementation of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

Internet Filtering

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to the IT/DSL.

All users have a responsibility to report immediately to the IT/DSL any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Internet Monitoring

To ensure that internet filters are performing as described in the policy IT will undertake regular monitoring (no less than once a week) of the Internet activity of users and that access to blocked content is not taking place. For example, a student has been able to access adult content or blocked social media sites.
The monitoring log should include:

- date monitoring took place
- Action taken to rectify any issues found in filtering process
- Any inappropriate activity should be logged and reported to the Network Manager.

Reporting: to ensure that unusual behaviour such as

- Searching for inappropriate content
- Extremist or radicalised content
- Content likely to have an impact on child's well-being – self harm, weight loss, drugs

is identified. The Designated Safeguarding Officer, HR admin and technical lead should agree the parameters for regular reports – daily, weekly, monthly – where frequency is dependent on how timely the information needs to be. The reports on student activity will be created by the DSL and HRA, with support from the technical lead where appropriate, and made available to staff as directed by the DSL. The reports on staff activity will be created by the HRA, with support from the technical lead where appropriate, and made available to staff as directed by the Principal.

In order to create an audit trail and prevent logs from being unopened, the receiver of the logs should record the date the report was checked, and any actions taken. This might include:

- Amending the report to reduce false positives
- Adding additional key words in search criteria
- Action taken when data indicates a person is at risk

Most logs will be a date followed by "no action taken".

All reports should be saved on the network for reference at a future point.

Policy Statements

Internet access is filtered for all users. Differentiated Internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and Internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

The reporting process alerts staff to unusual student online activity or possibly child protection issues. It is also a key element of the school's Prevent Strategy. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Any breach of the filtering policy will result in action in line with the United Learning Disciplinary Policy.
- The monitoring of the Internet filters is carried out regularly and failings in the systems is logged and reported to line manager.
- The Designated Safeguarding Officer or delegated staff will define appropriate filtering reports on student activity, in conjunction with technical staff, to identify online behaviours which might lead to child protection issues. These reports will be reviewed weekly, and actions logged.
- The HRA or staff delegated by the Principal will define appropriate filtering reports on staff activity, in conjunction with technical staff, to identify online behaviours which might lead to child protection issues. These reports will be reviewed weekly and actions logged.
- The school / Academy manages its own filtering service .
- The school has provided enhanced / differentiated user-level filtering through the use of the Trend Micro filtering programme, allowing different filtering levels for groups of users.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal (or other nominated senior leader).
- Mobile devices that access the school / Academy Internet connection (whether school / Academy or personal devices) will be subject to the same filtering standards as other devices on the Academy/ school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff and the E-Safety Officer. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through the Acceptable Use Agreement.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Any request for changes to the filtering system must be raised with the Network Manager, E-Safety Officer or any other IT technical staff. Requests must have a strong educational reason to be considered for unblocking of a site. All changes to the filtering system will be logged by Network Manager/IT technical staff and periodically reviewed by the E-Safety Officer.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager or IT technician who will decide whether to make school level changes (as above).

Additional Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the E-Safety Policy and the Acceptable Use Agreement.
Key logging software and screen capture will be used to monitor any E-Safety/Prevent Strategy or student welfare issues, as well as staff compliance with the Acceptable Use Policy.

Audit / Reporting

Logs of filtering change controls, filtering incidents and actions from filtering reports will be made available to E-Safety Officer / Police on request.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

Academy Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The Academy will be responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the Academy's policies).
- access to personal data is securely controlled in line with the Academy's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of Academy computer systems
- there is oversight from senior leaders, and these have impact on policy and practice.

Key Personnel

The Network Manager, members of SLT and the School Manager will be responsible for creating and reviewing the policy. This should be more than one member of staff as well as a member of the Governing Body.

Advice on Technical Security can be obtained from United Learning Central Office IT Support, European Electronic and Regional IT Technology Specialists.

Responsibilities

The management of technical security will be the responsibility of the Network Manager/Technical Staff/Principal and SLT.

Technical Security

Policy Statements

The Academy will be responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of Academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Academy systems and data. All such equipment is installed in locked rooms and cabinets, which are locked after use.

- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff which include the Network Manager and IT Support Staff.
- All users will have clearly defined access rights to Academy technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager/Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Members of IT Support are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Mobile device security and management procedures are in place with the use of an MDM.
- Academy technical staff regularly monitor and record the activity of users on the Academy technical systems and users are made aware of this in the Acceptable Use Agreement. Securus software presents the UAP at logon and monitors user activity.
- Remote management tools are used by staff to control workstations and view users activity. This is Net Support monitoring software.
- An appropriate system is in place through the IT Helpdesk for users to report any actual/potential technical incident to the E-Safety Coordinator/Network Manager/Technician (or other relevant person, as agreed).
- An agreed policy is in place (A guest login which allows basic access and storage) for the provision of temporary access of “guests” (e.g., trainee teachers, supply teachers, visitors) onto the Academy system. This takes the form of a visitor login providing access to the Academy internet and local storage but does not provide access to shared resources.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on Academy devices by users. This is controlled by the use of screen filters and filtering policies that deny the downloading and the saving of executable files.
- An agreed policy is in place (AUP) regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on Academy devices that may be used out of Academy.
- An agreed policy is in place (AUP) regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on Academy devices.
- The Academy infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc. Sophos Enterprise.

CCTV Policy

Introduction

Castle View Academy has in place a CCTV surveillance system "the CCTV system" across its premises. This policy details the purpose, use and management of the CCTV system in the Academy and details the procedures to be followed in order to ensure that the Academy complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

The Academy will conform to the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the Academy will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information' ("the Information Commissioner's Guidance").

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

This policy and the procedures detailed therein applies to all of the School's CCTV systems, webcams, covert installations and any other system capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. CCTV images are monitored and recorded in strict accordance with this policy.

CCTV System Overview

The CCTV system is owned by Castle View Academy, Allaway Avenue, Portsmouth, PO64QP and managed by the Academy and its appointed agents. The data controller for CCTV images held by Castle View Academy is United Learning Trust (ULT). ULT is registered with the Information Commissioner's Office (ICO). The registration number is Z7415170.

The Group's Data Protection Officer, Alison Hussain, is responsible for ensuring that ULT complies with the Data Protection Law. She can be contacted on company.secretary@unitedlearning.org.uk or 01832 864538.

The CCTV system operates to meet the requirements of the Data Protection Act 2018 and the Information Commissioner's Guidance.

Castle View Academy's designated Data Protection Lead is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

The CCTV system operates across the Academy. Details of the number of cameras can be given on request.

Clearly visible signs are placed at all pedestrian and vehicular entrances to inform staff, pupils, parents, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by the Academy and a 24-hour contact number for the Security Control Centre is provided, if appropriate.

The Data Protection Lead is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

Cameras are sited to ensure that they cover Academy premises as far as is possible. Cameras are installed throughout the Academy's sites including roadways, car parks, buildings (internal and external), within buildings and externally in vulnerable public facing areas.

Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screening or software masking will be utilised.

The CCTV system is operational and capable of being monitored for 24 hours a day, every day of the year.

Any CCTV installation shall be subject to a Data Protection Impact Assessment. It will also comply with the policy and procedures within this document. The Data Protection Impact Assessment shall be appended to this policy and shared with Central Office Data Protection Officer

Purposes of the CCTV System

The principal purposes of the Academy's CCTV system are as follows:

- for the prevention, reduction, detection and investigation of crime and other incidents (including vandalism);
- to ensure the safety of staff, children, visitors and members of the public and
- to assist in the investigation of suspected breaches of Academy regulations by staff or students.

The CCTV system will be used to observe the Academy's buildings and areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

The Academy seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy as outlined in the Privacy Impact Assessment.

Monitoring and Recording

Cameras are monitored in the Site Manager's office, which is a secure area, staffed during working hours.

Images are recorded centrally on servers located securely in the server room and are viewable in the Site Manager's office and the server room by all CCTV trained staff. Additional staff

may be authorised by the Principal to monitor cameras on a view-only basis to support trained staff i.e. in identifying specific children.

- Trained staff are as follows: David Nutland; Chris Bonner; Susan Blandford.

A log shall be kept of requests to access recorded images by staff and whether any recorded images have been copied to support specific investigations. Information logged should include: Name of staff, time and date of viewing, time and date of images reviewed, brief reason for viewing content (e.g. “incident in corridor”) but should not contain names, whether any images have been copied and where they have been copied to.

The cameras installed shall provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

All images recorded by the CCTV System remain the property and copyright of United Learning. The recorded images are stored onsite on a server. Downloaded footage used in investigations is securely stored onsite on a server, in accordance with the process outlined in the retention of images section.

The use of cameras placed in some of the classrooms to monitor student behaviour will be carried out in accordance with Part 3 of the Employment Practices Code.

The monitoring of classrooms should be clearly identified in the Privacy Impact Assessment. This should cover:

- identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver
- identifying any likely adverse impact of the monitoring arrangement
- considering alternatives to monitoring or different ways in which it might be carried out
- taking into account the obligations that arise from monitoring
- judging whether monitoring is justified

The CCTV system should not be used to carry out lesson observations.

The use of cameras in areas where one would normally expect a degree of privacy should be clearly identified on the Privacy Impact Assessment. This would include cameras placed in, or looking into, toilet or changing areas. Cameras should only be used in toilet or changing areas where there are full height cubicles, never in areas where it is possible to see people using the toileting facilities (excluding hand washing) or changing.

The use of covert cameras will be restricted to rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of both the Principal and Director of People will be sought before the installation of any covert

cameras. The Principal should be satisfied and be able to demonstrate that all other physical methods of prevention have been exhausted prior to the use of covert recording.

Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Compliance with Data Protection Legislation

From 25 May 2018, the Academy will also comply with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

All storage used for images, recorded or downloaded for investigations, must be in compliance with GDPR rules; on secure storage on premise or on cloud storage within the EEA

The existence of the Academy's CCTV system must be recorded in the Record of Data Processing Activities using United Learning's Education Information Portal (EIP).

Applications for Disclosure of Images

Applications by Individual Data Subjects

Requests by individual data subjects for images relating to themselves "Subject Access Request" should be submitted in writing.

In order to locate the images on the Academy's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

Where the Academy is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual. Any decision to withhold the requested images must be referred to the Group's Data Protection Officer or her team as there are specific rules that must be adhered to when applying the exemptions contained in the Data Protection Act 2018.

Access to and disclosure of images to third parties

A request for images made by a third party should be made in writing.

In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

All unexpected requests for CCTV images by third parties, including requests made by the police, should be referred to the Academy's Data Protection Lead in the first instance and if not available to the Group's Data Protection Officer or their team, who will advise on the application of any appropriate exemptions. Any third-party request should be added to the EIP in the GDPR area under *third party request*s.

Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/ Business Partner, the Principal may provide access to CCTV images for use in staff disciplinary cases.

The Principal may provide access to CCTV images to Investigating Officers when sought as evidence in relation to staff discipline cases.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

Retention of Images

Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

The automatic deletion of data after the defined retention period should be checked on a half termly basis. This should be logged on a half termly basis.

Where an image is required to be held in excess of the retention period referred to in 7.1, the Principal or their nominated deputy will be responsible for authorising such a request. A record of these stored images will be kept within the CCTV viewing log.

Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidential purposes will be deleted. The CCTV monitoring log will provide evidence of the images which have been held and where they are kept. When deleted this should be recorded in the CCTV monitoring log.

Access to retained CCTV images is restricted to the Principal and other persons as required and as authorised by the Principal. These individuals are: Dave Nutland, Sue Blandford and Chris Bonner.

Complaints Procedure

Complaints concerning the Academy's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Principal at Castle View Academy, Allaway Avenue, Portsmouth, PO64QP. Any complaint will be handled in accordance with the Academy's Complaints Policy.

All appeals against the decision of the Principal should be made in writing to the *Chair of Governors*.

Monitoring Compliance

All staff involved in the operation of the Academy's CCTV system will be made aware of this policy and will only be authorised to use the CCTV system in a way that is consistent with the purposes and procedures contained therein.

All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to have undertaken United Learning Data Protection training.

Policy Review

The Academy's usage of CCTV and the content of this policy shall be reviewed annually by the Principal and/or Governors with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

Password Policy

Overview

Usernames and passwords, sometimes referred to as 'credentials' are currently the predominant method of securing access to systems and resources across digital networks. A poorly chosen password may result in unauthorised access to, and exploitation of, United Learning's systems and data. Today the "passphrase" is fast becoming the norm to replace a simple password. For devices that do not support a password/passphrase other possibility using PIN codes etc are available. It is the duty of United Learning and all those responsible for overseeing its systems to implement a secure password policy locally and at the centre. There are three main risks which this policy attempts to mitigate:

- Data breach: Unauthorised access to school or Group systems could result in losing control of data and breaching the General Data Protection Regulation (GDPR). Failure to adhere to GDPR could lead to individual and corporate fines, unlimited compensatory payments, and reputational damage.
- Child Protection: Unauthorised access to school or Group systems could place children at risk, create embarrassment or otherwise invade their right to privacy.
- Operational disruption: Unauthorised access to school or Group systems could result in these systems or their data being made unavailable, impacting significantly on schools' ability to operate.

Purpose

The purpose of this policy is to define a strong password standard, establish best practice in the protection of those passwords and when they must be changed. The intent is to strike a balance between the two extremes of 'total lock-down' and 'completely open' to set a policy which ensures security whilst not creating burdensome barriers for authorised users.

Scope

The scope of the policy covers all staff and students who work or study in a United Learning school or Central Office location. This includes both United Learning Trust (ULT) & United Church Schools Trust (UCST) schools and sites.

Staff Policy

All staff who have, or are responsible for, an account that can access United Learning systems or data must use a password to protect this account. This password should not be shared/the same as any other password used on another system. This includes, but is not limited to, email accounts, management information systems (MIS), safeguarding systems, online learning portals, homework software and after school activity managers, etc.

Password/Passphrase Creation

- Standard user level passwords must contain a minimum of eight (**8**) characters (length should be as long as you can comfortably remember) and contain three of the following:
    - Lower case letter
    - Upper case letter
    - Number
    - Special characters e.g.!"$%^&*()¬
        - spaces are recommended as a special character (they increase the length)

    - avoid the £ sign – not all systems recognise it
- Passwords must not contain all or part of the user's name, username or other information known by others or easily discovered (e.g. pet or child's name, date of birth).
- Passwords should not be single words that are found in dictionaries. Phrases (combinations of 2-3 words) are encouraged which are memorable but less susceptible to brute-force automated attacks.
    - Pick a phrase that you can remember – The Quick Brown Fox – mix it up – thE Qu1cK br0wN F@x – a new long complex password is born (but don't use this one)!
    - Use character substitution (i.e. ! for 1, $ for S) sparingly – hackers are aware of this and will look for this in a password/phrase.
    - Spelling a word incorrectly – thE Qu1cK bBr0wN F@x – makes it more difficult for a hacker to use a dictionary attack.
- Passwords must not be re-used in multiple accounts. This exposes all accounts to breach should any one of them be compromised.
- Passwords used in personal accounts must not be used with United Learning accounts. To do so would make it easier for unauthorised users to access United Learning accounts via data shared from large-scale breaches of other systems (e.g. Gmail, Yahoo, TalkTalk).
- Passwords must not be characters or places from popular media (books, films TV programmes, etc) as these appear relatively high up the lists of most-frequently-used passwords.
- Passwords such as "Friday1!", "Password1", "Pa55w0rd", "Autumn2020", "Qwertyuiop" and "LetMeIn1234" are also poor choices, as they are common and exist in password dictionaries used by hackers and are sold cheaply on the dark web. Names of football clubs have been found in recent password hacks.
- The use of a password manager is advocated. With a single highly secure master password it is possible to store all relevant passwords, allow the generation of secure passwords and avoid using repeated passwords across multiple sites.
- Staff who have access to accounts with elevated privileges (accounts with access to more sensitive data, for example safeguarding information and students' health records, or which confer the right to make system changes) should take extra care when creating a password. The use of longer passwords and the use of special characters is required.
- Admin passwords used for accessing system level accounts should have a minimum of twelve (**12**) characters. Passwords for Admin accounts must have at least one of each of the following:
    - Lower case letter
    - Upper case letter
    - Number
    - Special character e.g.!"£$%#^&*(¬@>}~
- Admin accounts should only be used when carrying out admin tasks. It is best practice for admin level users to maintain a 'standard' account with a lower set of rights and a separate password, and to use this standard account for all general activity. Admin accounts should not have an email address associated with them where possible.

Password Change

- Standard user & elevated level passwords should be set to expire every 365 days (in better alignment with current guidance from the NCSC).
- Admin passwords must be set
    - to expire at (or within) sixty (**60**) days.
    - require MFA at pre-defined intervals.
- Systems must be configured to
    - inform users when a password is due to expire and how to change it.
    - prevent the re-use of passwords that have been previously used for the account.
    - prevent passwords from being changed more than once per hour.

Password Protection

- Staff should be given suitable training on the creation of strong passwords (see above under 0) and the need to keep these secure. This will ordinarily be part of annual Cyber Security Awareness training.
- Passwords must never be shared with anyone else, including IT Technicians, Line Managers, subordinates, or family members. There are procedures to allow assistants access to email and calendar accounts without compromising password security.
- Shared accounts (e.g., 'Reception PC') should not be used without prior authorisation from a suitably senior member of staff who understands the risks of doing this. Passwords for shared accounts tend to get written down and become common knowledge and the audit of which individuals have accessed an account is not possible. Shared accounts are a major vector of intrusion.
- Passwords must never be stored in plain text; this includes being written down on paper.
- If a user suspects that their password has been compromised, then they must contact the local IT Team immediately.
- Passwords must be unique and must not be used across systems/sites/suppliers; if the same password is used and is discovered this would allow multiple accounts to be breached (normally in a short space of time due to automated attacks).

Password Reset

- If a password is forgotten the user should use self-service password reset where it is available or contact the local IT Helpdesk to reset the password.
- If the user is not present a member of the local IT service may only communicate the new password using validated contact details found in the school's MIS, from HR or the employee's line manager.
- Reset Passwords should be set to expire on first use so that a new password can be entered.
- Passwords will not be sent to email accounts.

Password Vulnerability reduction

1. Use of Single Sign On (SSO) and Open Authorisation (OAuth) are encouraged for use wherever possible to reduce the exposure of passwords to other systems.

Account Lockout

2. Account lockout should be enabled such that an unacceptable number of attempts will cause the account to be locked out – either for a specific period or until it is unlocked by a system administrator.
3. Account lockout should be triggered after five incorrect attempts for staff and KS4 students where possible.
4. Account lockout for KS1-KS3 should be triggered between five and ten incorrect attempts.
5. Exceptions for staff may only be made after an appropriate risk assessment has been carried out and agreement from the Information Security Officer and the Head of Schools' IT Strategy is given.
6. Exceptions for students should be authorised at a local level by the Principal and must be documented by the Network Manager.

Mobile Devices

For mobile devices that do not support a password, other methods are acceptable:

a. PIN – a suitable PIN of 6 digits (or more if possible) – do not use your Date of Birth (or the Date of Birth of other persons known to you). Perhaps pick a historical date that has significance to you that you will be able to recall. Do not use a PIN you have used elsewhere.
b. Biometric – for devices that only you access and that you can enrol; be aware that a backup authentication method is strongly advised in the event that the biometric does not work (e.g., a fingerprint where there is interference (e.g., a cut) is unlikely to be recognised).
c. Finger/Iris print are acceptable biometrics
d. Facial recognition is susceptible to failure due to light conditions, use of glasses or other facial coverings.
e. Pattern – the use of a pattern is not acceptable as it is not secure and is very easy to guess (for example human nature is always to start at the top left corner of the pattern and there is a tendency to reproduce a number or a letter within the pattern). In addition, it has been proven that patterns are easier to determine at a distance.

Two/Multi Factor Authentication (2/MFA)

1. Initial sign up to 2/MFA must be done on site.
2. As stated above Admin level accounts must have 2/MFA enabled where possible. Service accounts with Admin privileges do not require 2/MFA but must have a long (20+ character) and complex password.
3. Staff with financial accountability and staff at an executive level must also have 2/MFA implemented as soon as possible; this will include but is not necessarily limited to Bursars/Business Managers/Registrars, Headteachers/Principals and Personal Assistants to Heads/Principals (because they will have access to much of the same information as the Heads/Principals. In addition, if 2/MFA is warranted by other factors (e.g. account/user has previously been phished, the target system has information deemed to be sensitive) then it should be implemented in line with other roles.
4. Normal user accounts will be required to use/have 2FA/MFA as soon as it is practical to do so.
5. 2/MFA can be implemented in a number of ways:

1. Using the school IP address range
2. Using an authenticator app
3. Use of a token
4. Use of a biometric
5. Using a key delivered using SMS or phone call

- It is for the school to determine the best factor to use (in consultation with Central Office staff).
- It is suggested that a SMS based 2 Factor is used only as a last resort – this is because it is, with the right knowledge (and sometimes equipment) it is easy to spoof or gain access to the message thereby rendering the 2nd factor ineffective.

Student Policy

All students at or above KS3 should be given password protected accounts. It is not absolutely required that students of primary age have complex passwords, as the sensitivity of the data in pupil accounts/ systems to which they have access is likely to be low. Pupil passwords will meet the criteria below.

Password Creation

- Students at KS1-2 should be encouraged to use and understand the reasons for named accounts with appropriate passwords. For practical reasons, complex passwords are unlikely to be suitable for younger students and a suggested password list, that increases in complexity as children get older will be made available. These passwords should not be used elsewhere, and different passwords should be used for credentials accessing other platforms such as Purple Mash, Times Table Rockstars etc.
- Pupil passwords at KS3 and higher must contain a minimum of eight (**8**) characters and contain at least one each of the following:
    - Number
    - Lower case letter
    - Upper case letter
- Special characters may be used
- Students should be given suitable advice on the creation of strong passwords and the need to keep these secure.

Password Change

- Pupil passwords should be set to expire every 365 days. KS1-KS2 passwords (used from the suggested password list) should be set not to expire.

Password Protection

- Students should be given advice not to share passwords with classmates or teachers.
- Passwords must not be stored by any member of staff, either in an encrypted or unencrypted form.

Password Reset

- Students should see their form tutor, a teacher, or IT Technical staff to get a password reset – whichever way is appropriate for your school. If self service is available a local decision can be made on its use.

Compliance

- Any adaptation of this policy must be approved in advance by the Information Security Officer.
- The Technology Specialists & the Information Security Officer will monitor the local adaptation and implementation of this policy through the Technology Assurance process.
- Any staff member failing to comply with their school or centre's password policy, for accounts that they are responsible for, will be managed in accordance with the United Learning Disciplinary Policy.
- School staff should do all that is practical to ensure that all applicable pupil accounts adhere to this policy.

Relevant Legislation

The Academy should be aware of the United Learning Policies and legislative framework under which this guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

United Learning Policies

- Child Protection Policy
- Safeguarding Policy
- Disciplinary Policy
- Bullying and Harassment Policy
- Whistleblowing Policy

Computer Misuse Act 1990

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.

Data Protection Act 1998

This protects the rights and privacy of an 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.

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.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

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 helpline staff.
- The organisation reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. Youtube).

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.

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.

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.

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 a 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

Sexual Offences Act 2003

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 fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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.

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 context of work with young people, 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 organisation is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Acceptable Usage of Technology - Guidance for Students

Academy Computers

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes (e.g. buying or selling goods).
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs, iPods, MP3 players etc.) unless you have the permission of the Systems Manager or the member of staff responsible for ICT.
- Do not eat or drink near computer equipment.
- Respect, and do not attempt to bypass security in place on the computers or attempt to alter the settings.
- If you are leaving your computer unattended for a short period, you might want to 'lock' your computer temporarily, rather than logging off and then logging on again. Press Ctrl + Alt + Delete keys at the same time and select lock computer. To unlock it simply enter your password.
- At the end of your session, you should log off, but do not shut your computer down or switch it off.
- The use of personal computing devices is bound by the Academy's Mobile and Other Electronic Devices Policy.

Internet (Academy computers and mobile devices)

- Do not access the Internet unless for study or for Academy authorised/supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive or hurtful to others, or which may bring the Academy into disrepute.
- Respect the work and ownership rights of people outside the Academy, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' or social networking activities over the Internet.
- Never arrange to meet anyone unless accompanied by a parent, guardian. People that you meet online are not always who they appear to be.

Security and Privacy (Academy computers and mobile devices)

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone that you connect with on the Internet your home address, telephone number or Academy name, or send photographs of yourself or others, unless you are given permission by a member of staff to do so.
- Do not use computers in a way that harasses, harms, offends or insults others.
- Computer storage areas, email conversations and removable media such as USB memory sticks, DVDs and CDs are treated like Academy exercise books. Staff may review files and communications to ensure that users are using the system responsibly.

Email (Academy computers and mobile devices)

- Be polite and appreciate that other users might have different views. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone that you know and trust. Attachments could contain viruses, which may destroy all the information and software on the computer.
- The sending or receiving of email containing material likely to be unsuitable for children or Academys is strictly forbidden. This applies to any material of a violent, dangerous, racist or inappropriate content.

Photographs and Video

- Do not take pictures or record film of any students or members of staff, while in Academy or on Academy trips, without the permission of those being photographed or filmed.
- If you need to photograph or film other students as part of an educational activity (e.g. drama rehearsal), you should use a Academy camera and you must seek permission from a teacher to make the film and check that students involved give their consent.
- Where personal devices are used, such as on Academy trips with general permission from the trip leader, consideration should be given to the appropriateness of uploading pictures or film to social media and if requested by the subject of the images, remove them from social media platforms. Uploading inappropriate photos or videos could result in disciplinary action.
- Never send, print, display or otherwise transmit images which are unlawful, obscene, abusive or hurtful to others, including ‘sexting’, or which may bring the Academy into disrepute.

Acceptable Usage of Technology Policy Agreement – Students

- You must read and sign this agreement before you can be allowed to use the Academy's ICT resources.
- You must agree to the Academy viewing on your Academy account, with just reason and without notice, any e-mails you send or receive, material you store on the Academy's computers, or logs of websites you have visited.
- You must only access those services you have been given permission to use.
- You must adhere to all instructions set out in the attached Guidance Document.
- You must also abide by the Academy's Mobile Devices Policy.
- If you become aware of a breach of this policy it is your responsibility to report it to a member of staff.

Penalties for misuse of computer systems will depend on the nature and seriousness of the offence. Disciplinary action may be taken against students who contravene this policy. The Academy, for various legitimate business practices, may need to monitor the use of e-mail and internet access from time to time for the following reasons:

- to establish the existence of facts (e.g. the details of an agreement made)
- to monitor for quality control and staff training purposes
- to prevent or detect crime
- to investigate or detect unauthorised use of the Academy's telecommunication system (including e-mail and internet)
- to intercept for operational purpose such as protecting against viruses and making routine interruptions such as forwarding e-mail to correct distributions
- to gain access to routine business communications (e.g. checking e-mail) when students are on holiday or sick leave

I confirm that I have read the Acceptable Usage of ICT - Guidance for Students, understand it and intend to comply with its obligations.

Full name (print) ……
Signature ……
Date ……

Acceptable Usage of Technology Policy Agreement - Staff

All employees must read and sign this Acceptable Use Policy before they can be allowed to use devices or services provided by or on behalf of United Learning. In signing this policy, you agree to the following:

- An authorised representative of the Group may view, with just reason and without notice or notification, any communications you send or receive, material you store on the Group's computers / services or logs of websites you have visited. This data, regardless of where hosted, belongs to United Learning at all times. It is the Group's policy not to view colleagues' emails without good cause.
- You will only access those services / aspects of services which you have been given permission to use.
- You will not use United Learning resources to operate your own business.
- You will not attempt to remove any of the security measures put in place by United Learning to ensure the integrity of its services, the security of its data or the appropriateness of employee activity.
- Any communication from a United Learning related account (email, social media) or account which identifies you as belonging to United Learning will be appropriate in tone and content.
- You will exercise caution when sending information via email to ensure that it is addressed to the correct recipient(s) and is the correct information (particularly when attaching documents). Personal data (that by which an individual could be identified) must not be transferred to other recipients unless encrypted or password protected, in line with the requirements of Data Protection legislation.
- You will not transfer United Learning data outside of the organisation's systems except via Group email or encrypted media. This includes the use of cloud storage and personal email accounts. *For example, saving files to Dropbox or emailing them to a personal Hotmail account may resolve logistical problems you are having but run the risk of those data leaving United Learning's control.*
- You will use the Internet and other services for appropriate activity only. United Learning considers inappropriate activities to include gambling (outside of workplace Lottery syndicates), pornography and sites promoting views which run counter to the organisation's ethos.
- You will not share your access credentials with anyone. Delegated access to calendars / email should be granted to administrative support staff, where required.
- You will not download, use, distribute or otherwise communicate any material which, in so doing, infringes copyright.
- The use of language deemed aggressive, offensive or intimidating is not acceptable. You must not write anything on a website or send by email or other medium anything which could be reasonably be deemed offensive.
- Use of a personal device to access any United Learning data is permitted, subject to the acceptance of the separate 'Bring Your Own Device' policy.
- Breach of this policy may result in disciplinary action.

Full name (print) ……

Signature ……

Date ……