# *SWINDON CLUSTER POLICIES*

## Technology Policy (S04)

### Why does a school or setting need a Technology Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

This Technology Policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and all computer and tablet technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care', which applies to everyone working with children.

There are a number of themes that run through all the policy areas addressed in this document. Firstly, there is the need to balance control against developing responsibility. Schools within United Learning must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. You must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions about how to use technology as well as to feel able to report any concerns.

Secondly there is a need to find a balance between a set of highly secure technology systems and usability. School leadership teams must be clear about how much freedom users should have and the risks these entail. Finally, there is the need to chart a sensible course to solve problems of misuse of technology; technical solutions can be used, for example to prevent student access of gaming sites during lessons but at heart these may be behaviour or cultural concerns that fundamentally should be tackled as such.

Breaches of the technology policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the consequences that inappropriate use of technology can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Principal and the Governing body.

The Technology Policy is essential in setting out how your school plans to develop and establish a safe approach to the use of Technology, to identify core principles which all members of the school community need to be aware of and understand, and to enable the school to develop an effective and safe online community.

### Scope

This policy applies to all members of the academy community (including staff, students / pupils, 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 policy applies to all schools, secondary, primary, independent and academies.

The Education and Inspections Act 2006 empowers the Principal to such an extent as is reasonable, to regulate the behaviour of students / pupils 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 school. 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 the 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 / Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor and it is combined with their role as Child Protection / Safeguarding Governor. The role of the E-Safety Governor will include:

- regular meetings with the Designated Safeguarding Lead
- regular monitoring of e-safety incident logs
- reporting to relevant Governors / Board / committee / 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 & Business Director.
- **The Principal and (at least) another member of the Senior Leadership Team (SLT) in each academy in the cluster 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 – in the appendix – "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 Principal & Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Executive Leadership Team (ELT) Senior Management Team will receive regular monitoring reports from the E-Safety Officer &/or Business Director.

### E-Safety Officer: Designated Safeguarding Lead (DSL), Alice Lawrence at Swindon Academy and Penny King at Nova Hreod Academy, assisted by Business Director, Sam Jadeja

- leads the e-safety reporting into the ICT Strategy Committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the academy technology policies / 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 / relevant body
- 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 Principal & E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of Governors
- reports regularly to Executive Leadership Team

### ICT Cluster Network Manager / Technical staff:

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 Local Authority / 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**
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Senior Leaders; E-Safety Officer for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

### 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 (SAUP)**
- **they report any suspected misuse or problem to the Principal / Senior Leaders ; E-Safety Officer for investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level** and only carried out using official academy systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the technology and acceptable use policies
- students / pupils 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 / pupils 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

### Child Protection and Designated Safeguarding Lead (DSL)

DSL should be trained in e-safety issues and be aware of the potential for serious child protection / 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 via ICT Strategy Committee

The ICT Strategy Committee provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding e-safety and the monitoring the technology policy including the impact of initiatives. Depending on the size or structure of the academy this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body via the E-Safety Officer.

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

- the production / review / monitoring of the academy technology policy / documents.
- the production / review / monitoring of the academy filtering policy (if the academy chooses to have one) and requests for filtering changes.
- 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 / pupils about the e-safety provision

## Students / Pupils:

- **are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to 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.
- should 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 parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. 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
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the academy (where this is allowed)

## Community Users

Community Users who access academy systems / website / VLE as part of the wider academy provision will be expected to sign a Staff Acceptable ICT Usage Policy before being provided with access to academy systems

## Breaches of the Policy

### By Students

Any breach of this policy may lead to disciplinary action being taken against the pupil/s involved in line with the academy's Disciplinary 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

| | |
|---|---|
| Mrs Ruth Robinson | Executive Principal |
| Mrs Alice Lawrence | Vice Principal and Designated Safeguarding Lead (DSL), Swindon Academy |
| Mrs Penny King | Vice Principal and Designated Safeguarding Lead (DSL), Nova Hreod Academy |
| Mrs Carol Shelley | Safeguarding Governor |
| Mrs Sam Jadeja | Business Director |
| Mr Scott Logan | Cluster ICT & Network Manager |

## Areas of risk

| | |
|---|---|
| Child Protection | Children are exploited by sex offenders<br>Children upload inappropriate content online<br>Children publish personal information which identifies them either overtly or covertly (location metadata in images or messages)<br>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<br>Staff lack of understanding of new online tools puts them at risk. |
| OFSTED Inspection | Lack of understanding of the e-safety policy by staff, students or governors can prevent the academy 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 and student should be via the staff academy email address only, this should be formal in nature and copied to the Student Record Inbox.

Using online services and sites, not provided by United Learning, to communicate between a teacher and a student may put one or both participants at risk. This is because; it is not open and transparent, there is no audit trail, United Learning do not control the communication channel so cannot access the data, it is impossible to monitor (even when it takes place in academy).

Staff are advised to use social networking sites with caution. Always be aware of their privacy policies. These can change frequently and can mean sharing of your personal data with other organisations. Staff are also advised not to allow students access to their private areas within these sites.

### 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 Computing / 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 are allowed to 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 Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and sanctioned by the class teacher.

## 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:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

## Education – The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's / academy's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk

## 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 SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

## Training – Governors / Directors

**Governors / Directors should take part in e-safety training / awareness sessions**, with particular importance for those who are members of any sub-committee / 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 (e.g SWGfL).
- Participation in academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

## E-safety Information

- **Internal & external resources**
  A useful link to reliable sources of information on the safe use of the internet, training resources, parental information sites, can be found on the academy and United Learning website as well as in the appendix to this policy.

## Reporting Procedures

- **Internal reporting**
  This should be reported using the internal online CPOMs reporting system. For Staff any concerns should be dealt with using the academy Safeguarding and Whistle Blowing 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, via the relevant Primary or Secondary Committee and technical information through the Finance & Premises Committee, ICT reporting.
- **External Reporting**
  The academy 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 Device 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, students are allowed to have their mobiles in their bags but they are not allowed to be used inside the academy building during the academy day. 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 such as iPhones, Blackberries, Android and Windows phones, and other 3G/4G and WiFi enabled devices such as iPads, iPods, tablets and laptops plus other similar devices not mentioned. 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 as part of the academy's Technologies Policy 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 academy, but their use is restricted as detailed in this policy.

This policy applies to all members of the academy community, including those in our EYFS setting.
This policy is reviewed at least annually by senior management, who will report to the Local Governing Body on its implementation on a regular basis.

In accordance with the academy's Provision of Information Policy, this policy is available on the academy's website and in hard copy from Reception. It should be read in conjunction with:

- Behaviour and Discipline Policy
- Anti-Bullying Policy
- Exclusions Policy
- Safeguarding 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 academy 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 common-sense 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

- **Students are not permitted to use mobile phones inside the building during the academy day, unless directed by a teacher in exceptional circumstances.**
- **3G/4G or WiFi enabled devices of any description, including mobile phones, iPods or iPads or similar mobile devices, must never be taken into public examinations by students or staff.**
- Mobile devices should be switched off during the academy day 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 a 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 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 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 behaviour policy. This may include confiscation until the end of the day and devices will only be returned if collected by a parent, or on a Friday if a pupil collects or longer for serious issues. For persistent offenders, phones will only be returned to parents. The academy will 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 or viewing inappropriate text or images. This could result in disciplinary action.

## Security of Mobile Phones and other electronic devices

**Students and staff are advised to have their devices security marked.**

The academy does not accept responsibility for mobile phones or other electronic communication devices or entertainment systems. Students should be advised to lock their devices in their lockers during lessons. 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 keep them in the staffroom, though their security there cannot be guaranteed.

## 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 – refer to staff bullying and harassment policy). In some circumstance's students may, for example, be asked to leave their mobile devices with the College Managers or other member of staff 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 member of SLT, College Manager or other member of staff will investigate the matter and report the matter to the DSL or Principal or Head. 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 in line with the **academy's search policy**. The student's parents may also be invited to attend the interview. It may be appropriate for the student to be excluded whilst the allegation is being investigated.

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 DSL, Principal or Head will be informed and the Police liaison officer. The mobile device will remain in the possession of the DSL, Principal or Head until advice from the police has been acted upon. This may include asking all students in possession of the image to delete it, if approved by the DSL or Principal. 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. If a formal disciplinary meeting is called, this will be in accordance with the procedure set out in the academy's policy on Exclusion, Expulsion, Removal and Review.

If the case of staff, any instances of inappropriate images of children or young people must be reported immediately to the Principal, or in her absence the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead.

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

**Staff working in the EYFS setting are specifically prohibited by EYFS regulations from using their personal devices (cameras, mobile phones) to take photographs or videos of children in the EYFS setting for any reason. Only academy devices may be used.**

With children in other years, the academy recognizes 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 the DSL, Principal or Head 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 site. The only exception is for the marketing department 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, Instagram or Twitter to e.g. to 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 Pupils

1) **Mobile phones are not allowed to be used during the academy day inside the building.**
2) All devices are brought into the academy at the pupil's own risk and the responsibility for their safekeeping lies with the pupil. The academy will take no liability for loss or damage.
3) The Academy is a place of work; pupils' 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.
4) Permission must be sought from a member of staff, and authorisation given, before a pupil may be allowed to use a mobile device on academy premises.
5) 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.
6) Any pupil 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. They should also expect to receive a detention.
7) If a pupil needs to contact home in an emergency, they must speak with a College Manager or another member of staff who will deal with the matter. Pupils should not contact home in the case of illness; this should only be done by a member of staff.
8) If parents need to contact pupils in an emergency, they should contact the academy reception and a message will be taken to the pupil. Parents are reminded that pupils should not have their devices turned on whilst on academy premises and, hence, will be unable to check for messages.
9) Pupils may only access the internet through the academy's network; no independent (for example through a 3G connection) access is permitted.
10) The accessing, or updating, of social media platforms is not permitted unless it is part of a structured educational activity.
11) The exception to the above is that pupils in the Sixth Form are allowed to use their devices only in their Common Room. If they use their devices outside of the Sixth Form Common Room, they should expect the same sanction as the rest of the academy.
12) Pupils 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 will lead to disqualification from that examination and potentially other examinations.
13) Pupils 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

1) 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.

2) 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 an accident occurred on the academy premises while under the supervision of a member of staff who could be proved to be using a digital device at the time of the accident, the academy may find itself liable. This would apply to activities both on and off the academy premises and would apply to any adult responsible for the supervision of students.

3) 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.

4) 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 pupil learning and cannot be sourced through the academy network (in which case, pupils should be made aware that the mobile device has been used for this educational purpose).

**5) Staff must not photograph or video pupils with a personal (mobile digital) device. If it is necessary to regularly take images of students for marketing purposes, then an academy owned device should be provided.**

6) Staff should endeavour to make any personal calls on their own mobile telephone, or similar, in a discreet fashion and away from any pupil area, for example in the Staff Room or in an office, behind closed doors.

7) Staff should not give out their personal mobile phone numbers, or other communication contact information, to students.

8) Inappropriate use of mobile devices is a serious offence; cases of misuse could lead to disciplinary action being taken against the individual concerned.

**APPENDIX 1 – Summary Points for Classroom Display**

- **Your device must be switched off at all times during the academy day whilst inside the building.**
- 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

### Introduction

The changing face of information technologies and ever-increasing pupil/ student 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 the academy by statute to search pupils 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 publicized 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 a 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, whether privately or academy owned, 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.

Each academy publicize their behaviour for learning policy all year round on their school website.

### Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The Academy Behaviour (Determination and Publicizing 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 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: Senior Leadership Team, Curriculum Leaders and College Managers, ICT & Network Manager and Technology Team. No data should be deleted without authorisation from the DSL, Principal or Head.

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:

The academy Behaviour for Learning Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. 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 each academy in the mobile device policy:

- At Swindon Academy: Electronic and mobile devices must be switched off at all times during the school day whilst in the academy buildings.
- At Nova Hreod: Electronic devices and mobile devices must be switched off at all times during the school day whilst in the school grounds.

**If students breach these rules:**
The sanctions for breaking these rules can be found in the mobile devices policy.

Authorised staff (defined in the responsibilities section above) 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 pupil's consent for any item.
Searching without consent - Authorised staff may only search without the pupil'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 / pupil is in possession of a prohibited item i.e. an item banned by the academy 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/ pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student / pupil 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 / pupil 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 (i.e. the 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 break the academy rules).

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 inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of academy discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:**

- **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**

Care should be taken not to delete material that might be required in a potential criminal investigation. The academy provides access to a Confidential Care line for staff member who need support after undertaking a search and accessing disturbing images, information can be provided by the HR Officer.

## 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.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of academy discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

## 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.

## Audit / Monitoring / Reporting / Review

Where a search is required full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files through the B4L or alternative behaviour system and subsequent CPOMs Safeguarding recording system.

These records will be reviewed by the E-Safety Officer or Business Director at regular intervals, every two weeks, and reported to the Principal and E-Safety Governor as part of the termly Child Safeguard reporting process.

This policy will be reviewed by the Principal and governors annually and in response to changes in guidance.

# Social Media Policy

## Introduction

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 and maintaining pages on internet encyclopaedias 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 pupils 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

Alice Lawrence, DSL at Swindon Academy and Penny King, DSL at Nova Hreod Academy will overseas the implementation of this policy supported by Sam Jadeja, the Business Director, and Scott Logan, the Cluster 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 the 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 encyclopaedias (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.

Academies 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**

Each Academy maintains a presence 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 is used to collate and publicise a stream of positive messages about the multitude of activities that go on at the academy 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, subject to approval by the Principal or Head.

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

- services such as Twitter 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**. User names should be formal (e.g. @MrSmith_AcademyName) or anonymised (e.g. @PEAcademyName). 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 Vice Principal (DSL) or 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 pupil's tweeted question confirms that pupil 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. 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 pupils 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 post inappropriate content to a social media platform with their consent or knowledge. The consequences can be long term and damaging.

A member of staff leaves their iPad in the classroom and is picked up by a student. Seeing he can access the staff member's twitter feed he proceeds to post racist comments. He is also able to change the password and email account associated with the twitter feed. He does not take the iPad. It takes 2 days for the member of staff to get the account deleted, during which time more comments have been added and seen by a significant number of parents, pupils and other professionals.

While out for an evening a friend picks up your phone and writes some "witty tweets" while you are at the bar. They do not reflect you as a member of staff and make people question your professional judgement. The same is possible on email and other communication platforms.

## 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**

1 **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).

Someone may have created your academy as location on Facebook, or other location-based service. In checking yourself into academy one day you would then be identified with the academy.
By adding academy as an employer on Facebook it may be possible for people to search for all employees of the academy at a future point, irrespective of your privacy settings.

2 **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. For example, that photograph of Friday night at the end of term could, once commented on or liked by one of your direct contacts – the second party, be visible by multiple third parties over whom you have no control.

3 **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 a 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 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

4 **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 academy to be compromised.

5 **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 Director of ICT/ Head teacher/ appropriate delegated leader.

6 **Staff members must decline 'friend requests' from pupils they receive to their personal social media accounts**. Instead, if they receive such requests from pupils 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.

7 **On leaving the academy's/ United Learning's service, staff members must not initiate contact with former pupils by means of personal social media sites whilst that pupil is under the age of 18**. It is likely that any ex-pupil will have children from their old academy as friends. In accepting

the friend request the content you post, are tagged in, or comment on, may become visible to children in your academy.

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

9 **Information 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.**

10 **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**.

11 **Staff members must not edit open access online encyclopaedias 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.

12 **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 work place.

13 **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**.

14 **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.**

15 **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 on line 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 Bullying and Harassment 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 other**s. If photographs are taken at a Swindon Cluster 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 a Swindon Cluster 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/Group 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 a Swindon Cluster 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, a Swindon Cluster Academy does not deem this as appropriate behaviour. If you receive a request from a child / young person / mother / father / carer / then 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 in line with the information set out in section 5 of this policy.
- **Discuss work related issues online**. This takes into account conversations about child / young person / mother / father / carer / colleagues or anything else which may identify a Swindon Cluster Academy 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.
- **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 Swindon Cluster Academy's 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 a Swindon Cluster Academy or 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. Cyber bullying and what it means is set out in the Bullying and Harassment policy and procedure.
- **Post derogatory, defamatory or offensive comments** about colleagues, the children / young person / mothers / fathers / carers, your work, a Swindon Cluster Academy or United Learning. 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.

## Filtering, Monitoring and Reporting 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 and which could potentially put students and staff at risk. 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 following policy aims to keep up with this fast pace by documenting roles, responsibilities and procedures that the academy will put in place.

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 academy 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 academy.

Many users are not aware of the flexibility provided by many filtering services at a local level for academies.

### Key Personnel

The Governors will ultimately be responsible for the policy.

- The Senior Leadership Team & Business Director will be responsible for creating and reviewing the policy in conjunction with the Principal and Cluster ICT & Network Manager.
- The ICT team will provide educational and technical expertise on Internet filtering, monitoring and reporting, supported by the United Learning Technology Business Support Team.
- The ICT & Network Manager will be responsible for generating reports on student internet activity, reviewed by the Principal, DSL's and/or Business Director each term.
- The ICT & Network Manager will be responsible for generating reports on staff internet activity, reviewed by the Principal, DSL's and/or Business Director each term.

United Learning and Impero can provide educational and technical expertise on Internet filtering.

### Responsibilities

The responsibility for the implementation of the academy's filtering policy will be held by the Cluster ICT & Network Manager. They will manage the Swindon Cluster 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 academy filtering service must

- **be logged in change control logs via the helpdesk function**
- **be reported to a second responsible person**, the Business Director**:**
- be reported to and authorised by a second responsible person, Principal, Business Director or DSL prior to changes being made
- be reported to the ICT Strategy Committee every term.

All users have a responsibility to report immediately to Cluster ICT & Network Manager any infringements of the academy'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 the Cluster ICT & Network Manager will undertake regular monitoring 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, blocked social media sites or sites promoting radicalisation.

The monitoring log includes:

- date monitoring took place
- Action taken to rectify any issues found in filtering process
- Any inappropriate activity should be logged and reported to Vice Principal (DSL).

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 Principal, Designated Safeguarding Lead, Business Director and Cluster ICT & Network Manager will agree the parameters to create fortnightly reports on student activity. These will be created by the Cluster ICT & Network Manager and shared with the DSL, Principal and Heads of each phase as appropriate. These reports will be and made available to other staff as directed by the VP (DSL). The reports on staff activity will be created by the ICT & Network Manager and shared with the Principal and Business Director and made available to other staff as directed by the Principal.

All reports should be saved on the network in G:\Admin\ICT\Monitoring\ for reference at a future point. If a serious breach is identified it must be reported to the Principal immediately.

## Policy Statements

Internet access is filtered for all users. Differentiated Internet access is available for staff and customised filtering changes are managed by the academy. 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 academy 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 academy'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 academy network, filtering will be applied that is consistent with academy 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 are logged and reported to the ICT & Network Manager and/or Business Director
- The Designated Safeguarding Lead 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 monthly and actions logged
- The Principal 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 monthly and actions logged or immediately when an alert is generated through the filtering system.

- The academy has provided enhanced / differentiated user-level filtering through the use of the filtering programme. Thus allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc. 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 Business Director.
- Mobile devices that access the academy Internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the academy systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list should be made through the ICT helpdesk and considered by the ICT & Network Manager & referred to the DSL and/or Business Director. If the request is agreed, this action will be recorded and logged through the ICT helpdesk. A summary of such actions shall be reviewed regularly by the ICT Strategy Committee.

### 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
- induction training
- staff meetings, briefings, Inset.

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

### Changes to the Filtering System

- Students may request changes to the filtering system through teaching /support staff. Staff may request these changes through the ICT Helpdesk.
- Changes will only be made if there is a strong educational reasons for the changes to be made.

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 ICT & Network Manager who will decide whether to make academy level changes (as above).

### Monitoring

Swindon Cluster Academy supplement the filtering systems with additional monitoring from Impero, which monitor all text typed or displayed on screen and flag inappropriate content, language & images.
No filtering system can guarantee 100% protection against access to unsuitable sites. The academy/ academy will therefore monitor the activities of users on the academy network and on academy/ academy equipment as indicated in the E-Safety Policy and the Acceptable Use Agreement.

### Audit / Reporting

Logs of filtering change controls, filtering incidents and actions from filtering reports will be made available to:

- the Principal, DSL and the Business Director
- ICT Strategy Committee
- E-Safety Governor / Governors committee

- SLT & College Managers as required
- External Filtering provider / Local Authority / Police as required 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.

## Academy Technical Security Policy (including passwords)

### 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 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 Cluster ICT and Network Manager, members of SLT and Business Director will be responsible for creating and reviewing the policy.

### Responsibilities

The management of technical security will be the responsibility of the Cluster ICT and Network Manager .

## 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 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 the 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, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained.**
- **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 ICT Strategy 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 the ICT 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.
- 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.
- Remote management tools are used by staff to control workstations and view users activity.
- An appropriate system is in place through the ICT 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 / pupils / 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.
- Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

## Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all academy technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

### Policy Statements

- All users will have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- **All academy networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the academy systems, used by the technical staff must also be available to the Principal or other nominated senior leader and kept in a secure place e.g. academy safe. Consideration should also be given to using two factor authentication for such accounts**.
- **The academy should never allow one user to have sole administrator access**
  Passwords for new users, and replacement passwords for existing users will be allocated by ICT Support Staff. Any changes carried out must be notified to the manager of the password security policy (above).
- All users (adults and young people) will have responsibility 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.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below
- The level of security required may vary for staff and student / pupil accounts and the sensitive nature of any data accessed through that account)
- Requests for password changes should be authenticated by Library Staff or ICT support staff to ensure that the new password can only be passed to the genuine user. For staff this request will need to be authorised by the individuals line manager or a member of SLT and by a member of staff for a request by a pupil student.

### Staff passwords:

- **All staff users will be provided with a username and password** by ICT Support team who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of academy
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous (e.g. the last four passwords cannot be re-used) passwords created by the same user.
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised

- should be different for systems used inside and outside of academy

### Student / pupil passwords

- **All users will be provided with a username and password** by ICT Support staff who will keep an up to date record of users and their usernames.
- Users will be required to change their password every new term (old term).
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.
- Student passwords can be rest by Library Staff or ICT Support Staff to the student username, which will then require a reset at first login.

### Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the academy's password policy:

- at induction
- through the academy's e-safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the academy's password policy:

- in lessons as part of ICT induction
- through the Acceptable Use Agreement

### Audit / Monitoring / Reporting / Review

The responsible person, ICT & Network Manager, will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy will be reported to a member of Staff, ICT Support staff.

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

### 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.

## Appendix A
## Acceptable Usage of Technology - Guidance for Pupils

### Academy Computers

1) Do not install, attempt to install or store programs of any type on the computers without permission.
2) Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
3) Do not use the computers for commercial purposes (e.g. buying or selling goods).
4) 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 ICT & Network Manager or the member of staff responsible for ICT.
5) Do not eat or drink near computer equipment.
6) Respect, and do not attempt to bypass security in place on the computers or attempt to alter the settings.
7) 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.
8) At the end of your session you should log off, but do not shut your computer down or switch it off.
9) The use of personal computing devices is bound by the academy's Mobile Device policy.

### Internet (academy computers and mobile devices)

1) Do not access the Internet unless for study or for academy authorised/supervised activities.
2) 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.
3) Respect the work and ownership rights of people outside the academy, as well as other students or staff. This includes abiding by copyright laws.
4) Do not engage in 'chat' or social networking activities over the Internet.
5) 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)

1) Do not disclose your password to others, or use passwords intended for the use of others.
2) 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.
3) Do not use computers in a way that harasses, harms, offends or insults others.
4) 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)

1) Be polite and appreciate that other users might have different views. The use of strong language, swearing or aggressive behaviour is not allowed.
2) 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.
3) 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**

1) Do not take pictures or record film of any pupils or members of staff, while in academy or on academy trips, without the permission of those being photographed or filmed.
2) If you need to photograph or film other pupils 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 pupils involved give their consent.
3) 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.
4) 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 – Pupils

1) You must read and sign this agreement before you can be allowed to use the academy's ICT resources.
2) 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.
3) You must only access those services you have been given permission to use.
4) With the permission of your Class Teacher and the ICT & Network Manager you may bring your own portable devices such as laptops into academy and you will be able to access the internet, using academy Wi-Fi, but will not have direct access to resources stored on the academy network.
5) You may **not** bring personal storage devices such as USB 'memory sticks' into academy.
6) You must adhere to all instructions set out in the attached Guidance Document.
7) You must also abide by the academy's Mobile Devices policy.
8) 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 pupils 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 pupils are on holiday or sick leave

**I confirm that I have read the Acceptable Usage of ICT - Guidance for Pupils, 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 policy before they will be issued with log-on details and given permission to use computer equipment, handheld devices and or other services provided by, or on behalf of United Learning Trust (ULT).

Swindon Academy computing resources are provided primarily to facilitate a person's essential work as an employee, student or other role within the Academy. Use for other purposes, such as personal e-mail or recreational use is a privilege, not a right and as such can be withdrawn at any time. Any such use must not interfere with the user's duties or any other person's use of computer system and must not, in any way, bring the academy into disrepute.

Any malicious alteration or inappropriate use of the computer equipment may result in denial of service for other users and so the following rules of usage must be read, understood and adhered to at all times.
All employees must read and sign this Acceptable Use Policy before obtaining access to devices or services provided by, or on behalf of United Learning. By signing this policy, you are agreeing to the following:

a. That an authorised representative or specifically designated employee 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, servers/cloud and web browser history to ascertain the nature and detail of internet searches you have made and websites and/or pages you have viewed. This data, regardless of where hosted, is the intellectual property of, (belongs to), United Learning at all times. It is the group's policy not to view colleagues' e-mails without good cause.
b. You will only access the services and aspects of services which you have been given permission to use. This will vary depending on your job role.
c. You will not use the equipment and resources of United Learning to operate your own business.
d. You will not remove or attempt to remove any of the security features or measures put in place by United Learning. They exist to ensure the protection and preservation of the service provision, to enhance the security of personal data belonging to employees and other staff and to facilitate the monitoring of appropriate activity while using the computer equipment, its software and the network.
e. Any communication from a United Learning account, actual or sub-related (such as e-mail, exchange or any other social media platform) which identifies you as belonging to United Learning must be conducted in the appropriate tone, with content relevant to the age range of the students on roll.
f. You must exercise caution when sending information via e-mail 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 the Data Protection Act.
g. 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 e-mail 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.***
h. You will use the Internet and other services for appropriate activity only. United Learning considers inappropriate activities to include, but are not limited to, any illegal activity, gambling (outside of workplace Lottery syndicates), pornography and sites promoting views which run counter to the organisation's ethos. Failure to comply with this could result in formal disciplinary action being taken.
i. You will not share your access credentials (e.g. usernames, passwords or memorable data) with anyone. Delegated access to calendars\email should be granted to administrative support staff, where required.

j. You will not download, use, distribute or otherwise communicate any material which, in so doing infringes copyright.
k. The use of language deemed aggressive, offensive or intimidating is not acceptable and a zero tolerance approach is applied to this. You must not write anything on a website, send an e-mail or any other document in any format or language, which could be deemed offensive by another person, whether this was the intention, or even directed towards the person who takes offence.
l. 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."
m. Any breach of this policy may result in disciplinary action being taken.

---

**I confirm that I have read and understood the Acceptable use of Technology Policy-Staff Agreement and agree to comply.**

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

## Appendix B – OFSTED Guidance

### Introduction

Inspectors have been given guidance on inspecting e-safety. It will not be possible to gain a Good or Outstanding if academies do not have an effective Technology Policy in place.

**OFSTED report "Inspecting e-safety 2013" highlighted indicators of inadequate practice**

- Personal data is often unsecured and/or leaves academy site without encryption.
- Security of passwords is ineffective, for example passwords are shared or common with all but the youngest children.
- Policies are generic and not updated.
- There is no progressive, planned e-safety education across the curriculum, for example there is only an assembly held annually.
- There is no internet filtering or monitoring.
- There is no evidence of staff training.
- Children are not aware of how to report a problem.

Inspectors have guidance on questions to ask students, staff, governors and parents on the effectiveness of the e-safety policy on academy – do students know how to report concerns, when were staff last trained, what input have governors had into the policy.

**OFSTED report "Inspecting e-safety 2013" recommended that academies:**

- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at academy
- use pupils' and families' views more often to develop e-safety strategies
- manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at academy and the more open systems outside academy
- provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- work with their partners and other providers to ensure that pupils who receive part of their education away from academy are e-safe
- systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.

### Staff Training

Regular staff training is necessary to enable staff to keep up to date with the latest changes in both technology and trends in online tools used by adults and children alike.

- Initial training for all staff
- Annual update training for staff (maybe as part of new academic year training) Recommended by OFSTED
- Training for e-safety staff (this should be more than one member of staff) and how it can be cascaded

### Student Education

E-safety should be firmly embedded in the academy curriculum. The e-safety policy should reference when it is, and what is, delivered within the Computing Curriculum, PSHE and across the curriculum, as well as events such as Safer Internet Day. Some academies will integrate it into Anti-Bullying week in October as well.

### Community Training
The policy should state what training is offered to parents and how often it is delivered. This might include information on parental e-safety evenings, information send home to parents and information posted on online portals

### New Technologies
The use of multiple devices such as tablet, smart phones, laptops and computers to access the internet, online resources and social media platforms provide a challenge for all academies, their staff and their students. There is a need therefore to constantly update the training to enable all of the academy community to staff up to date with these changes.

### Reporting
What processes are in place to enable students to report issues or concerns, either about their own online behaviour or about others? This might be pointing students to external organisations such as CEOP or Childline, or to internal reporting mechanisms such as a specific email address, online form on the academy website or individuals to approach.

### Monitoring
The academy will need to outline how it monitors all elements of the e-safety policy

- How is the effectiveness of student education measured
- How is the effectiveness of staff training measured
- How effective is the community training measured
- How many incidents have been reported and how were they dealt with
- Reference to the Internet Filtering Policy

### Internet Filtering
The Internet Filtering Policy is a separate policy but should be referenced in the e-safety policy.

**OFSTED's "Inspecting e-safety**

**Sample questions for academy leadership**

How do you ensure that all staff receive appropriate online safety training that is relevant and regularly up to date?

| | |
|---|---|
| Why this question? | The Ofsted report *The safe use of new technologies*[1] (February 2010) concluded that staff training is a weak area of online safety provision. The South West Grid for Learning (SWGfL) report *Online Safety Policy and Practice*[2] concluded, based on feedback from 1500 UK academies via '360 degree safe', that staff training is consistently the weakest area of academies provision. |
| What to look for? | at least annual training (in-service or online) for all staff<br>training content updated to reflect current research and advances in technology<br>recognised individual or group with e-safety responsibility |
| What is good or outstanding practice? | one or more members of staff have a higher level of expertise and clearly defined responsibilities |

What mechanisms does the academy have in place to support pupils and staff facing online safety issues?

| | |
|---|---|
| Why this question? | SWGfL concluded in their sexting survey (November 2009)[3] of 1,100 11–16 year olds, that 74% would prefer to report issues to their friends rather than a 'trusted adult'. The Department or Education (DfE) report *The use and effectiveness of anti-bullying strategies* (April 2011)[4] refers to multiple reporting routes, consistent whole academy approach, good auditing processes and regular self-evaluation. |
| What to look for? | robust reporting channels |
| What is good or outstanding practice? | online reporting mechanism, nominated members of staff, peer support |

How does the academy educate and support parents and whole academy community with online safety?

| | |
|---|---|
| Why this question? | Marc Prensky (2001)[5] coined the expression, 'digital natives' and 'digital immigrants', describing the 'generational digital divide' (Byron 2008)[6] that exists between children and their parents. Only 33% of European parents had filtering software on their computers.[7] |
| What to look for? | Parents' e-safety sessions<br>raising awareness through academy website or newsletters |
| What is good or outstanding practice? | workshops for parents<br>regular and relevant e-safety resources offered to parents<br>children educating parents |

[1] *The safe use of new technologies (090231),* Ofsted, 2010; http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies.

[2] *Online safety policy and practice in the UK and internationally – An analysis of 360 degree safe/Generation Safe self review data 2011*, SWGfL & Plymouth University, 2012, http://www.swgfl.org.uk/Staying-Safe/Files/Documents/Online-Safety-Policy0-and-Practice-in-the-UK-and-in.

[3] *Sharing personal images and videos among young people*, SWGfL & Plymouth University, 2009; http://www.swgfl.org.uk/Staying-Safe/Sexting-Survey.

[4] *The use and effectiveness of anti-bullying strategies in schools*, Department for Education (DfE), 2011; https://www.education.gov.uk/publications/eOrderingDownload/DFE-RR098.pdf.

[5] Digital Natives, Digital Immigrants – A new way to look at ourselves and our kids; Marc Prensky, 2001; http://marcprensky.com/articles-in-publications/

[6] *Safer children in a digital world: the report of the Byron Review* (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.

[7] Livingstone, Olafsson, O'Neill & Donoson, *Towards a better internet for children*, London School of Economics (LSE) 2012; http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx

Does the academy have e-safety policies and acceptable use policies in place? How does the academy know that they are clear and understood and respected by all?

| | |
|---|---|
| Why this question? | The SWGfL report *Online safety policy and practice*[8] concluded that most academies consistently report having such policies in place, however very few have policies that are produced collaboratively, are linked to other policies, and are reviewed frequently. |
| What to look for? | e-safety policy is regularly reviewed<br>evidence that these are freely available (poster, handbooks, etc)<br>children can recall rules |
| What is good or outstanding practice? | children integral to policy production |

Describe how your academy educates children and young people to build knowledge, skills and capability when it comes to online safety? How do you assess its effectiveness?

| | |
|---|---|
| Why this question? | A key recommendation in the Byron review (2008)[9] was building the resilience of children to online issues through progressive and appropriate education. |
| What to look for? | planned and progressive e-safety education programme delivered across all age groups |
| What is good or outstanding practice? | e-safety is embedded throughout the academy curriculum and is regularly reviewed |

**Sample questions for pupils**

1. If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
2. If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
3. Can you tell me one of the rules your academy has for using the internet?
4. Can you describe the risks of posting inappropriate content on the internet?

**Sample questions for staff**

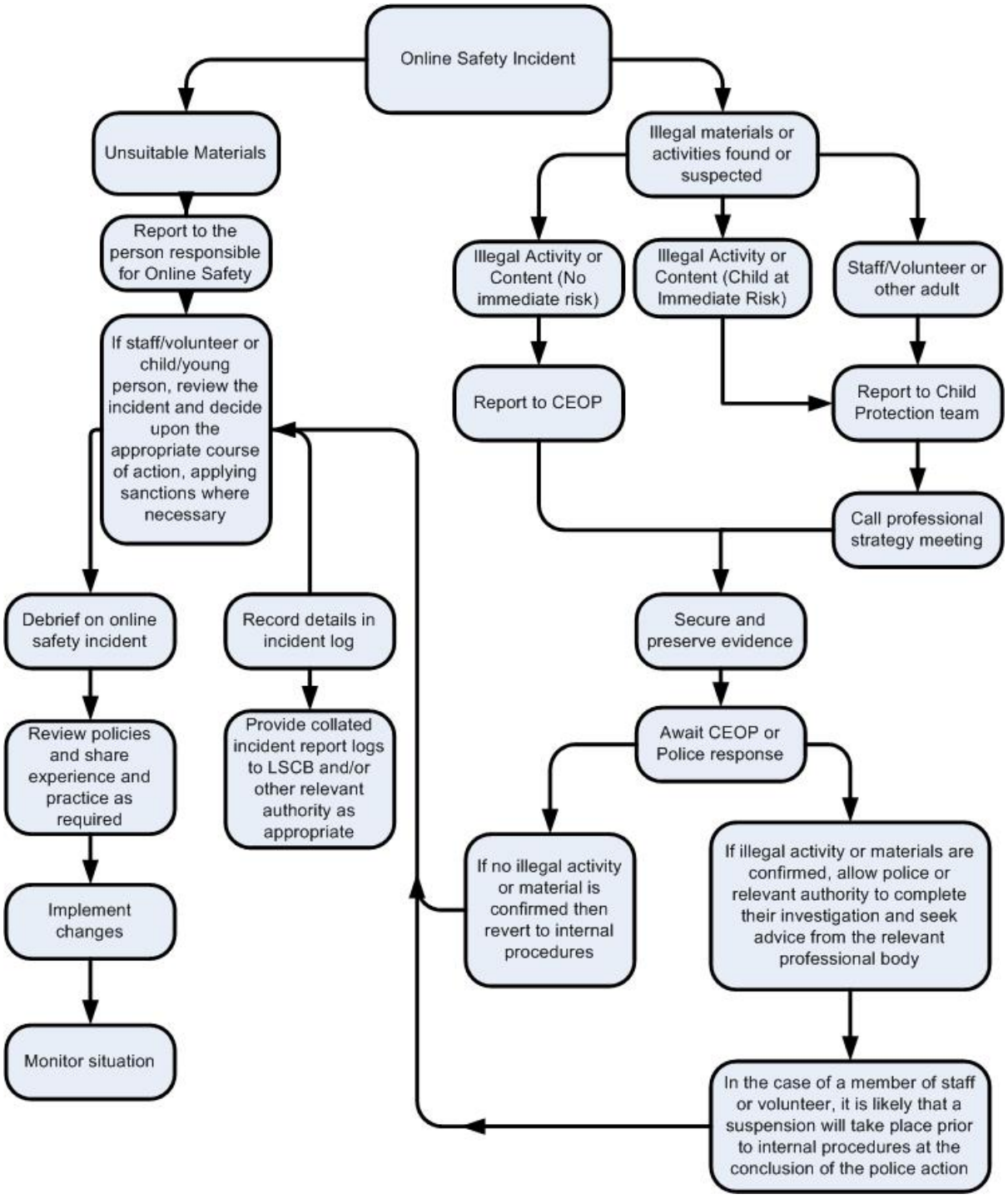
1. Have you had any training that shows the risks to you and pupils' online safety?
2. Are there policies in place that clearly demonstrate good and safe internet practice for staff and pupils?
3. Are there sanctions in place to enforce the above policies?
4. Do all staff understand what is meant by the term cyber-bullying and the effect it can have on themselves and pupils?
5. Are their clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?
6. Does the academy have any plans for an event on Safer Internet Day? (This is an annual event, now in its fifth year at least, so academies that participate will know about the event).

In a good academy we should expect positive answers to all of the above. It would demonstrate a academies commitment to e-safety if all staff had received some awareness training outlining what the current risks are and what resources are available to help them keep pupils and themselves safe online.

[8] *Online safety policy and practice in the UK and internationally – An analysis of 360 degree safe/Generation Safe self review data 2011*, SWGfL & Plymouth University, 2012.

[9] *Safer children in a digital world: the report of the Byron Review* (PP/D16(7578)/03/08), DCSF and DCMS, 2008.

## Appendix C – Responding to Incidents of Misuse – Flowchart




Taken from the SWGFL - Responding to incidents of misuse – flow chart, part of their E-safety Academy Template Policies Document.