

# INFORMATION SECURITY POLICY

<b>Policy Type</b>	
<b>Adopted by</b>	<b>Trustees</b>
<b>Chair of the Trustees</b>	<b>Rev Nigel Sinclair</b>
<b>Date</b>	<b>16.07.2018</b>
<b>Reviewed</b>	<b>23.05.2019</b>
<b>To be reviewed</b>	<b>23.05.2022</b>

### **Aims:**

Elevate Multi Academy Trust (Elevate) and its Academies:

- are committed to the protection of information and administrative resources, including paper and electronic resources and the media in which they are stored or transmitted;
- will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed;
- will make every effort to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- will ensure all personal data is obtained fairly in accordance with the “Privacy Notice” and lawfully processed;
- will ensure confidentiality, information will be protected against unauthorised access and only authorised personnel will modify it;
- Will ensure security measures such as encryption and password protection for electronic media are in place;
- Will ensure secure storage for hard copy material is provided to protect against theft or loss;
- Will ensure staff will receive training and guidance to enable them to understand, and appropriately apply, security measures for the protection of all information.

References to the Head Teacher includes the Head of School and Executive Head Teacher.

### **Legislation and Guidance:**

- GDPR 2017
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 2000
- Education (Pupil Information) (England) Regulations 2005. This may include sharing personal data where it is fair and lawful to do so.
- The Telecommunications Act 1994
  - DFE: Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers. July 2018
  - DFE: Draft non-statutory guidance for school leaders, school staff, governing boards and local authorities November 2018
  - Keeping Children Safe In Education 2018

### **Links with other Trust Policies and Practices:**

Elevate Acceptable Use of ICT policy  
Elevate Data Protection policy  
Elevate Data Retention policy  
Elevate Bring Your Own Device policy  
Elevate On line Security policy  
Elevate Child Protection and Safeguarding policy

Elevate Behaviour policy  
Elevate Searching screening and confiscation policy  
Elevate Complaints policy  
Elevate Lap top agreement

### Responsibility:

**The Chief Executive Officer (CEO):** has responsibility for the implementation of this policy and the management of information security across Elevate.

**The Data Protection Officer** has overall responsibility for monitoring / maintaining this policy and accompanying guidance and providing advice and guidance on implementation.

**The Head teacher** is the Senior Information Risk Owner for their respective Academy and have day to day responsibility for managing information security within the Academy.

**Staff:** are responsible for implementing the policy in their areas of responsibility.

: It is the responsibility of every employee to adhere to this policy.

This policy and the accompanying guidance will be reviewed, and if necessary updated, every three years.

### Security and Care of Equipment:

- All items of equipment are the property of Elevate and as such must be kept well maintained and secure at all times;
- If a member of staff wishes to borrow a piece of equipment, (a laptop, for example) full details will be recorded by the Office Staff;
- If the equipment is lost or stolen then the Head teacher and the Police must be notified immediately. If the equipment was being used for processing personal data then the procedures given below (Security of data) should have been followed to ensure the data was kept safe from disclosure;
- All equipment should be proprietorially marked using an approved security marker to aid identification if recovered, following theft or loss. An asset register which lists all equipment should be kept by the Academy Office – this should include a list of identifying information such as equipment ID's.

### Security of Data:

- Elevate has a statutory duty under **the Data Protection Act** to ensure appropriate technical and organisational measures are taken to protect personal data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- All staff should ensure that any electronic or paper documents which contain personal data or, are otherwise confidential, are protected against unauthorised access. This includes ensuring that paper records are securely locked away, not just at the end of the day but when staff are out of the office, and that when staff are away from a computer it is switched off, or locked against access and password protected.

- Where computers hold personal or confidential data they should be password protected. Any memory sticks or removable devices used to store personal data, or used by staff away from the Academy, should be password protected and encrypted. Staff should not use their own personal memory sticks or removable devices for work purposes and **MUST NOT** use private equipment to store personal data.
- The primary copy of Academy information should never be stored at home, so Academy records should be updated as soon as possible with copies of any work that staff do at home, and the home copy deleted.
- Staff must also take reasonable security measures to protect the information they take home from unauthorised loss, access or amendment. Whenever possible, staff should ensure that copies of Academy information are not stored on their private PC, including in temporary directories.
- When taking paperwork home, staff should ensure that it is stored securely when not in use and is not vulnerable to theft, or accidental access by family members.
- Information in transit should be protected by being locked in a briefcase or car boot.
- Memory sticks and similar are easily lost or mislaid and should be carried securely (not in a pocket or on a lanyard). Staff should avoid transferring information or equipment from a car interior to a car boot in a car park where the car will subsequently be left, or leaving information or equipment in a car or car boot at any time when the car is unattended.
- Servers and back-up systems should be kept securely in locked cabinets or a locked area to which only staff have access. Similarly, hardware such as laptops which are kept at the Academy should be locked away at the end of the day, not left on desks or visible through windows.
- Use of emails, scanners or fax systems to transfer data should be limited according to the sensitivity of the data being transferred. Staff must always check that information is being sent to the appropriate recipient. It is strongly suggested that to send sensitive personal data staff use recorded delivery mail which can be tracked or delivered by hand if encryption facilities are not available.
- Staff should not share or give out passwords and should not permit anyone without clearance to access secure information.
- **The Computer Misuse Act** makes it an offence to access any computer system for which access authorisation has not been given. Thus any attempt to interfere with or try to bypass the security controls on a computing system is an offence. Similarly trying to obtain information, such as users' passwords or accessing or modifying files belonging to other people who have not given access authorisation is also an offence.

### **Secure Disposal:**

All confidential waste paper should be shredded and / or disposed of through a confidential waste service. This includes personal data due for destruction, duplicates of personal data and other confidential information.

Computer systems must be fully cleansed of any information before they are disposed of or re-sold. Approval and support for this must be obtained from the DPO/Premises manager. Discs, memory sticks and other removable devices should be destroyed if they are intended for disposal.

### **Security of Buildings:**

All staff must wear ID badges. Staff should be prepared to challenge any member of the public within the Academy to ensure that they have a right to be there.

Any contractor should carry identification and show this on request. All contractors will need to sign in and sign out at the office.

Staff should ensure that windows and external doors are locked when a classroom or office is empty, and at the end of school, and that offices, filing cabinets and cupboards are also kept locked if required.

Any security concerns including break-ins and loss of computer equipment must be reported to the Head teacher and the Police.

### **Email Security:**

Staff must bear in mind that email is a formal record of correspondence and can be subject to request under Data Protection and Freedom of Information legislation – emails are also retained as records on staff, children and school files.

Staff must not send anything which would be unlawful or discriminatory, or whose content is defamatory or libellous. Work emails should not be used for forwarding chain letters or similar 'spam'. The Telecommunications Act 1994 makes it an offence to transmit messages or other matter via a public telecommunications system that is indecent, obscene or menacing. This includes causing annoyance, inconvenience or needless anxiety to another by a message that the sender knows to be false

If members of staff receive an email which breaches Elevate's policies or breaks the law they are advised to speak to a senior staff member of staff or the DPO/Premises manager before responding. This includes 'spam' emails, particularly those purporting to be from banks, or any email asking the recipient for money.

Staff should re-read any message before sending, checking for clarity and content (including grammar), and ensure that the message is being sent to the appropriate recipient.

Do not use email if the information being sent is personal or confidential, unless you are certain the information will be secure for example through password protection.

Do not use email to anyone who is known not to check emails regularly, or where a phone call or meeting would be a more appropriate way to get the message across.

Do not use email where there may be a contractual or legal need to provide a written and signed document or prove the identity of the sender.

### Internet Security:

Access to the Internet must be used responsibly and legally. Staff must not take *any* action which could bring Elevate and its Academies into disrepute, cause offence, interfere with the organisation's work or jeopardize the security of data, networks, equipment or software.

Under no circumstance should staff make use of the Academy internet to access chat lines or similar services.

With the advent of e-commerce, staff should beware of committing the Academy to purchase or acquire goods or services without proper authorisation. Purchase order must be raised for all goods and services **with Elevate's Finance Manager**.

Staff must not attempt to download or install unauthorised software from the internet.

Staff should be aware that, as with paper sources, not all information on the internet is accurate, complete or reliable. Users should ensure its validity, as they would printed publications, before using it.

At any time and without prior notice, Elevate reserves the right to examine e-mail, personal file directories, and other information stored on Elevate's network and equipment. Permission to examine such information will only be granted by the Chief Executive Officer.

### Security of Records:

Access to data, and particularly personal data, should be limited to staff who have a genuine 'need to know'. Staff should be aware that all computer systems permit audit trails to be checked to see who has altered or updated data.

Changes to data, and particularly personal data, should be carried out promptly and recorded appropriately so the reason for the change and its originator is known.

Records should be properly managed to enable staff to find or identify information quickly and accurately. Best practice dictates that children and staff records are kept in one location – multiple locations will lead to duplication or discrepancies between files.

### Reporting & Responding to Security Breaches:

In the event of a suspected data breach we will follow the procedures detailed in Elevate's Data Protection policy and Appendix 1.

A security breach would be caused when [and this not an exhaustive list]:

- A laptop containing personal data is lost or stolen;
- A USB [memory stick] containing personal data is lost or stolen;
- A vehicle containing a laptop or paper files is stolen;
- A laptop or paper files are stolen from a private property;
- An email is sent [either internally or externally] with files attached containing personal data and the email is sent to the wrong email address;

- An email is sent [either internally or externally] with files attached that contain personal data which is far in excess of that necessary in order for the business function to be carried out;
- An email is sent [either internally or externally] which should be sent “bcc” to a large number of people, is instead, sent “to” and so the recipient is aware who else has received the email and their personal email address or other personal details;
- Personal data is shared outside of the Academy for a legitimate business reason, but it is lost by the recipient, or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for;
- Personal data is transferred electronically outside the Academy and is not encrypted when it should be;
- Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose;
- A member of staff uses personal data for a personal rather than an Academy or Elevate business reason.

Any theft from the Academy should be immediately notified to the Police and DPO.

Any loss of or damage to technical equipment should be notified to the **DPO/Premises manager.**

The Data Protection Officer for cases involving breaches of IT security will investigate the security breach / loss of data through the process detailed at **Appendix 2**. The investigation will determine whether to notify the Information Commissioner Officer. The following guidance will be followed when considering a referral to the Information Commissioner [Notification of data security breaches to the ICO](#)

### Copyright:

Ensuring Licensing and Copyright requirements are met is challenging. As part of the government’s commitment to reducing the administration burden on state academies in England the DFE has **funded** agreements to purchase copyright licenses centrally.

The following copyright organisations are now held centrally and therefore the following licences are provided and funded centrally for state funded academies:

#### **Copyright Licensing Agency (CLA)**

CLA licenses organisations to copy and re-use extracts from print and a wide range of digital publications on behalf of the copyright owners – authors, publishers and visual artists. The term ‘Copying’ means the reproducing of an original work by means of photocopying or making digital copies of content from magazines, books, journals, electronic and online publications. CLA licences provide a cost effective way of managing the risks associated with using and reproducing copyright materials.

Contact details: [academies.cla.co.uk](http://academies.cla.co.uk) / email: [education.customers@cla.co.uk](mailto:education.customers@cla.co.uk) / tel: 020749003100

#### **The Educational Recording Agency (ERA)**

Era licenses designated educational establishments to record radio and television broadcasts for educational purposes. This also includes the licensing of access to digital recordings for use on interactive whiteboards, VLEs and PowerPoint presentations. Licences to copy and transmit for curricular purposes PRS for Music repertoire of copyright music by

means of recording broadcasts containing music and communicating such recordings from academies to teachers and pupils at the school are covered by Education Recording Agency's licence or top up licence. A top-up licence (Era Plus) is required for streaming recordings off-site (top up licence, if required, to be purchased by the school from ERA as it is not included in those provided centrally by DFE)

Contact details: [www.era.org.uk](http://www.era.org.uk) / email: [era@era.org.uk](mailto:era@era.org.uk) tel: 02078373222

### **Christian Copyright Licensing International (CCLI)**

CCLI is the UK's major licensing body for the reproduction of hymns and worship songs used in acts of collective worship during assemblies. CCLI licenses academies to reproduce the lyrics and music of many thousands of songs by hand, type, computer, storage and photocopying or use on OHP acetates, electronic storage and projection and song sheets

Contact details: <http://academies.ccli.co.uk> / email: [info@ccli.co.uk](mailto:info@ccli.co.uk) / tel: 01323436100

### **Photographic Performance Limited (PPL)**

PPL licenses recorded music played in public and broadcast on TV, Radio and the internet on behalf of the record company and performer members. A PPL licence is required for any public performance of recorded music for extra-curricular purposes within academies, such as school discos, keep fit classes etc. PPL licences can be obtained from The Centre for Education and Finance Management (CEFM)

Contact: PPL - [www.ppluk.com](http://www.ppluk.com) / email [ppo@ppluk.com](mailto:ppo@ppluk.com) / tel: 02075341070

CEFM - [www.cefm.co.uk](http://www.cefm.co.uk) / email: [ppl@cefm.co.uk](mailto:ppl@cefm.co.uk) / tel: 01494 836233

### **The Performing Rights Society (PRS)**

PRS licenses organisations to perform in public (whether live or by the showing or playing of sound recordings, films or broadcasts) and to communicate to the public (including intranet or internet transmission) the copyright works of its members and overseas societies. A PRS for Music licence is required for any public performance of music for extra-curricular purposes within academies. Licences can be obtained from PRS for Music's agent CEFM. Some commercial uses of music may need to be licenced directly by PRS for Music or by other members.

Contact – CEFM (refer to contact details above)

PRS for Music – [www.prsformusic.com](http://www.prsformusic.com) / email [customerservice@prsformusic.com](mailto:customerservice@prsformusic.com) tel: 0845 3093090

### **Motion Picture Licensing Company (MPLC)**

MPLC Umbrella Licence gives academies complete access to premium entertainment content from the majority of Independent, family friendly, film Studios/TV series DVD. The licence allows unlimited showings, in any legal home entertainment format and also provides single title licensing for film clubs.

Contact – [www.mplcuk.com](http://www.mplcuk.com) / email: [ukinfo@mplc.com](mailto:ukinfo@mplc.com) / tel: 01323649647

### **Film bank Media - Public Video Screening License (PVSL)**

PVSL was created by Filmbankmedia who represent all major Hollywood plus Independent and Bollywood studios. The licence enables academies to show films for entertainment purposes during and out of school hours, including in after school and film clubs.

Contact - [www.filmbankmedia.com/licences/](http://www.filmbankmedia.com/licences/) email:[pvsl@cefm.co.uk](mailto:pvsl@cefm.co.uk) / tel:01494 836231

**Newspaper Licensing Agency (NLA Media Access)**

NLA media access grants rights to academies to make copies of articles from the print and digital newspaper titles. NLA media access has appointed CLA as its exclusive agent for all UK education licensing.

Contact - [education.customers@cla.co.uk](mailto:education.customers@cla.co.uk) / tel: 02074003124

**Academies Printed Music License (PMLL/ SPML)**

The licence permits the copying of works from UK printed music publications that the school owns for use in school activities. The SPML is available exclusively from CLA.

Contact – Academies Printed Music Licence / email: [education.customers@cla.co.uk](mailto:education.customers@cla.co.uk) / tel: 02074003124

**In addition to the above** the following licence can be obtained, if required:

PRS for Music as MCPS licenses the copying of music onto CD, tape, video or DVD or other sound-bearing medium, including online platform, and the distribution of such copies to the public. This applies to recordings of school concerts, plays or similar events. Applications for MCPS licence can only be made on the website.

Contact – [www.prsformusic.com](http://www.prsformusic.com)/ email:[applications@mcps.co.uk](mailto:applications@mcps.co.uk) / tel:02083787500

Also top-up licences identified above may also be required to be purchased by academies as these are not included in the centrally funded licences.

**Detailed information in relation to copyright and licensing**

The following information identifies what the above licenses allow, including quantities and situations, where appropriate:

**Photocopy, retype or scan text or images to display electronically (IWB, VLE, OHP) from an original hard-copy book (CLA licence).*****In a lesson***

If the school owns the publication you can copy or display:

- one complete chapter from a book
- one short story or poem not exceeding 10 pages in length from an anthology
- 5% of the publication, if greater than above
- 1 article or 5% of the article within a journal or periodical

***As part of Extra Curriculum***

- Authorised persons can reproduce copyright material from books owned by the school when on site and within the school's secure IT network, this includes teachers, pupils and their parents, other school staff and governors.

**Photocopy, retype or scan text or images to display electronically (IWR, VLE, OHP) from an original journal or periodical (CLA Licence)*****In a lesson***

If the school owns the original publication, you can copy or display

- One article from a magazine, journal or periodical
- 5% of the publication, if greater than above.

***Extra-Curricular Use***

- Authorised persons can reproduce copyright material from magazines, journals and periodicals owned by the school when on site and within the school's secure IT network, this includes, teachers, pupils and their parents, other school staff and governors.

**Photocopy, retype or scan text, images or an entire cutting to display electronically (IWB, VLE, OHP) from an original newspaper (NLA media access Licence)**

***In a lesson***

- Make hard copies of print newspaper cuttings
- Make electronic copies of print newspaper cuttings
- Make electronic copies of digital newspaper cuttings
- Make hard copies of digital newspaper cuttings

***Extra- Curricular Use***

- Limited to copying and circulating cuttings for educational purposes usually taking place within the school premises

**Photocopy, retype or scan music or lyrics to display electronically (IWB, VLE, OHP) from original hardcopy sheet music (Academies Printed Music Licence)**

***In a lesson***

- Make copies of entire works from UK printed music publications that the school owns  
It DOES NOT cover:
  - Choral leaflets with a paper cover and less than 32 pages long
  - Use for private music lesson in which pupils are taught instrumental or vocal technique
  - More than 10% of the items (pieces of music or songs) included in the anthology or large vocal score (eg one out of ten songs, rather than 10 pages from a 100 page anthology)
  - Any works specifically excluded by a publisher – a list of exclusions is available on the CLA website
  - Copying of music for collective worship is excluded. Licences for this purpose can be obtained from CCLI

***In collective worship / assemblies (Christian Copyright Licensing International (CCLI))***

- Create service sheets/handouts which contain song words, create OHPs, project onto a screen
- Create customised arrangements of music where no published version is available

**Make copies of text and/or images from an online magazine, journal or website or from born digital resources eg eBook or CDROM (CLA Licence)**

***In a lesson***

To make copies then the CLA website tool should be used to check

<http://academies.cla.co.uk/about-your-licences/documentscla-licence/licenceddocuments> .

Other sites will have their own terms and conditions which you MUST check before using their content.

***Extra-Curricular Use***

- Authorised persons are able to reproduce copyright material from opted-in online content that the school owns or subscribes to when on site and within the school's secure IT network. This includes teachers, pupils and parents, others school staff and governors.

**Make copies of a digital audio file, such as music, sound-clip, interviews, audio-books, lectures eg mp3, mwa, wav, cda, RM, quicktime (ERA Academies Licence)**

***In a lesson***

- Radio broadcasts – permission is granted under the ERA academies license (if you are unsure what you want to do is covered then check on to record and use radio broadcasts)

## **Making copies of a digital audio file, such as music, sound clips, interviews, audio books, lecture etc**

### ***In a lesson***

- Radio broadcast – permission is granted under the ERA academies license and can be used within teaching, including providing copies for students (if you unsure what you want to do is covered then check on [www.era.org.uk/whatlicense](http://www.era.org.uk/whatlicense))
- No blanket licence is available for the use of other audio files used in the course of instruction – if you wish to use an audio file that is neither a radio broadcast nor a music file, you will need to check the copyright information and seek permission from the producer of the original work if you wish to use the resource outside of the stated restriction

### ***Extra – Curricular Use***

- Other – as above

## **Make copies of a digital video file, such as video file downloads eg AVI, Mpeg, flash, RM, mp4 etc**

### ***In a lesson***

- Digital TV broadcast: Permission is granted under the ERA Academies Licence. All on-demand services state that content is intended for personal use only, which does not include showing broadcast material during a lesson. However, BBC iplayer and Channel 4 On Demand have adapted their terms for educational establishments that hold an ERA licence, permitting the use of the content in the course of educational instruction. This also covers the use of recordings of television broadcasts and download it for use in teaching (including making available to students), If unsure whether what you want to do is covered, contact ERA directly on [era@era.org.uk](mailto:era@era.org.uk)
- Film/ Video – No licence is required for use of film used in the course of instruction. Pre-recorded films, on home entertainment formats (Video, BluRay, Digital File, AVI, MPEG, Flash, RM, MP4 etc) whether rented or purchased or downloaded from the internet are intended for home use only, as per Copyright, Designs and Patent Act 1988. Showing films anywhere outside of a domestic, home environment are all considered 'public performances' and require a licence from the copyright owner.

Other additional points to note:

- Copies of pre-recorded DVD/ Videos are illegal and therefore for concurrent use academies would need to purchase a number of copies of the film
- Copying any embodied musical works – films / videos may contain (embody) musical works within them, you require additional permission to make a copy

### ***Extra-Curricular Use***

- Film / Video, including Music Video – the terms of purchase of the resource may already include the required licences. There are two elements to consider:
  - Copying the film – licences are readily provided by the industry, with each licence offering specific rights for the type of location and event and it is important that teachers/ activity managers select the right licence
  - Pre-recorded films, on home entertainment formats follow regulations in line with the requirements identified for use in lessons (see above)
  - The Public Video Screening Licence (PVSL) was created by Filmbankmedia (representing many major film studios and distributors including Warner Bros, Sony Pictures, Disney, 20<sup>th</sup> Century Fox, Universal, Paramount Pictures, MGM and many more. The PVSL is available on an annual basis and enables academies to show films from participating studios for entertainment purposes during and out of school hours, including during extra-curricular activities. The MPLC Umbrella Licence® is an annual licence to screen unlimited films from the studios/distributors in the MPLC

repertoire throughout the year to a non-paying audience. Film clubs and PTA's can also be licensed on a fee per title basis. Contact MPLC.

- Copying any embodied musical works – films/ videos may contain (embody) musical works within them, **and in such cases require additional permissions to make a copy of them**

#### **Make copies of music, videos or films to transmit to others eg via academies' intranet**

- You will need to obtain permission from the publisher if you wish to transmit images of printed music, your own recorded performance, videos or films, and/or record company if you wish to transmit a copy of a commercial recording (PRS for music and PPL may be able to advise you of who you need to contact or whether you require an additional licence)

#### **Make copies of sheet music, music notation or lyrics from a born digital format**

- Sheet music, notation and/or lyrics – the Academies Printed Music Licence permit the copying of entire works from UK printed music publications that the school owns. It does not cover Choral leaflets with a paper cover and less than 32 pages long, use for private music lessons for pupils, more than 10% of the items included in an anthology or large vocal score, any works specifically excluded by a publisher, and music used for Collective worship (see below for more information in relation to some of these)
- Chord-sheet or lead-sheet for a hymn and/ or worship song for use in Collective Worship/ assemblies will most likely be covered by CCLI. In all other instances, if a school wishes to make copies from a digital original, permission must be sought directly from the music publisher. The Academies Printed Music Licence permits the reproduction of works only from printed music publications.
- Care needs to be taken when using music from the internet – in all cases (even if the copyright symbol is not displayed) checks need to take place regarding exceptions or is unsure contact should be made to check permissions rights

#### **Make copies of video or film or audio recordings of music to play or perform**

##### ***In a lesson***

- The PRS for Music Limited Manufacture (LM) licence grants the permission for the repertoire they represent. If the music or recording is not controlled by PRS for Music you may require permission directly from the rights owners. PRS for Music do not control music that is out of copyright. PRS and PPL offer a joint Limited Manufacture (LM) licence granting the permission required for the Music repertoire they represent.
- Permission will also be required from the record company or record label in order to copy a music video, and permission from the film distributors in order to copy feature film soundtracks which embody the 'original musical works'
- PRS for music and PPL represent the vast majority of commercially available music that is most likely used in academies. Where the music is out of copyright then certain permissions to make copies will not be required, but in the case of other music not covered by PRS or PPL then permission will be required from the rights owners

##### ***Outside of the Curriculum***

- The PRS for Music Limited Manufacture (LM) licence grants the permission required for the repertoire they represent.
- If the music or recording is not controlled by PRS for Music you may require permission directly from the rights owners
- PRS do not control music that is out of copyright
- Permission from the record company or record label to copy a music video and permission from the film distributors to copy a feature film

- Film soundtracks that embody the 'original musical works' are required to be separately licenced by the copyright owner

### **Make copies of music to play or perform**

#### ***Outside of the curriculum***

- The terms of purchase of the resource may already include the required licences. PRS for Music and PPL offer a joint Limited Manufacture (LM) licence granting the permission required for the repertoire they represent.
- PRS for Music and PPL also represent the creators of the vast majority of music that is likely to be used in school.
- Where the Music or a recording is out of copyright you may not require certain permissions to make copies or if it is not controlled by PRS for Music or PPL you may require permission directly from the rights owners (PRS for Music or PPL may be able to advise you regarding this).

#### ***At a school activity***

- The Academies Printed Music Licence permits the reproduction of printed music for school activities such as concerts, recitals and other performances
- The licence requires the school to include a credit on all copies
- More information can be obtained from Academies Printed Music Licence

#### ***Extra-Curricular***

- A licence for Music from PPL and PRS is required if you wish to use music (CDs, records, MP3 files etc). Both licences are available from CEFM (Centre for Education & Finance Management [www.cefm.co.uk](http://www.cefm.co.uk) tel 01494 459183)
- Third party (eg people hiring the school premises) playing music may also require separate licences from PRS for Music and PPL
- If, in the unlikely event that all the music you play or perform (outside the curriculum) is either not in copyright or not controlled by PRS for Music and PPL, you will not require their licences
- For film tracks which embody the 'original musical works' the right to perform or play these works must be separately licensed by the copyright owner, normally PRS for music.

### ***Collective Worship/ Assemblies***

- Permission is granted under the CCLI Licences
- The Collective Worship Music Reproduction Licence (CWMRL) from CCLI permits you to photocopy music from hymnbooks and worship songbooks. The licence is supplementary to the Collective Worship Copyright Licence (CWCL) from CCLI.

### **Watch all or part of a film**

#### ***In a lesson:***

- No licence is required for use of films in a lesson, for educational purposes if the audience is limited to teachers, pupils and other directly connected with the curriculum activities of the establishment. This does not, however, permit to the editing or adapting of any part of a film.

#### ***Extra- Curricular Use***

- Permission is granted under the PVSL and MPLC licences. This excludes pre-recorded films on home entertainment formats (refer to previous section number)
- Film soundtracks embody the 'original musical works' and the right to perform or play these works **must be separately licensed by the copyright owner.**

## **Play a radio or TV broadcast**

### ***In a lesson***

- Permission is granted under the ERA Licence. This licence allows use of programmes or clips from recordings originally made from television or radio broadcasts and Teaching presentations using BBC online services (iPlayer), Channel 4 on demand and ITV on demand services (to check for more information [www.era.org.uk/the-licence/faq](http://www.era.org.uk/the-licence/faq) and [licencing@era.org.uk](mailto:licencing@era.org.uk))

### ***Extra-Curricular Use***

- Permission is granted under the PPL and PRS Licences

## **Play or perform music**

### ***As part of a lesson***

- No licence is required to play or perform music as part of a lesson

### ***On school premises***

- A PRS (Public Performance Sales) licence from PRS for music is required if music is played on school premises (this is not covered by the Radio licence above as this does not give permission to play music or own broadcasts in offices or studio)
- A PRS Licences is also required if a short term RSL is being broadcasted for an event

## **Sourcing of Music**

Note the following guidance on the use of electronic formats of music:

- Legally purchased downloads on condition that the usage complies with the Digital Rights Management (DRM) rules accompanying the download eg, if the download is restricted to being held and played back from a specific PC or MP3 player, the public performance has to be sourced from that PC or MP3 player. If the download rules allow the track to be burned to a CD, that CD can then be used for public performances in the same way as any conventional commercial CD
- Licensed streamed from non-interactive internet radio services (this would include the Internet broadcasts of licensed commercial radio stations such as Capital, XFM etc, as well as internet-only radio services that have the correct licences in place).

## **Student/ School Radio**

- In addition to the webcaster licence from PPL, if a radio station is only accessible online then a Limited Online Music Licence (LOML) will be required from PRS for Music
- The Long Term Radio Licence (Long term RSL) is required from PRS for Music for student/ school radio services broadcasting within their school via hard-wired or intranet transmissions. To qualify for this an application must be submitted to OFCOM
- Short Term Radio Licences (Short term RSL) can be provided by PRS for student / school radio services that wish to operate an AM/FM transmission. This licence is restricted to 28 consecutive days. To qualify for this an application must be submitted to OFCOM
- Both the Long Term Radio Licence and the Short Term Radio Licence are a joint PRS and MCPS Licence. The licences allow OFCOM-licenced restricted service stations the right to broadcast PRS-controlled repertoire and record MCPS-administered repertoire. There are some restrictions in relation to music used in advertising or station idents. Full terms and conditions can be found on the PRS for Music Website.

## **Creating a multi-media resource to use**

- Permission to use copyright content is granted under the following licences – CLA, NLA media access, ERA, PPL, PRS, CCLL, PVSL, MPLC, SPML
- The same terms apply in a mixed-media resource as with other educational uses of copyright material, whether using a work in its entirety or just a clip or extract (refer to licence requirements in relation to the relevant resource)

- Text and still images from books, journals, magazines and websites – remember to check the Terms and Conditions of content that find on the intranet
- Newspapers – NLA media access has appointed CLA as its exclusive agent for all UK education licencing
- The NLA Academies Licence permits a academies to a) make hard copies of print newspaper cuttings b) make electronic copies of print newspaper cuttings c) make electronic copies of digital newspaper cuttings d) make hard copies of digital newspaper cuttings
- School staff can distribute newspaper cuttings to pupils, parents, staff and governors
- NLA media website provides additional information on using newspapers in the classroom, as well as a database of newspaper clippings that can be downloaded ([www.newspapersforacademies.co.uk](http://www.newspapersforacademies.co.uk))
- If a school uses digital Cuttings for purposes other than teaching or receive a press cuttings service, an extension to the Licence and Digital Fee may apply (contact NLA for advice)
- TV / Radio broadcasts – the ERA licence allows academies to use extracts from TV or radio broadcasts, including embedding clips into resources made using presentation software, such as Powerpoint or interactive whiteboard package
- Film – you are not permitted to edit or adapt any part of a film. Film clips require a special licence provided by the studios individually. Film soundtracks which embody the 'original musical works' permission to perform or play, copy or transmit these works must be separately licensed by the copyright owner.

### Events Licensing:

Organisations who want to carry out licensable activities on their premises must have a license or other authorisation from a licensing authority – usually the Local Authority.

The relevant licenses are:

#### ***Temporary Event Notice (TEN)– for one off events***

Licensable activities include:

- Selling alcohol
- Serving alcohol to members of a private club
- Providing entertainment eg music, dancing or indoor sporting events
- Serving hot food or drink between 11pm and 5am

A TEN is also required if the organisation already has a licence but wishes to carry out an activity which is not currently included in their licence.

The TEN only covers events which have fewer than 500 people (including staff) and lasts for no more than 168 hours (7 days). There are regulations regarding the number of TENs an organisation can have in any one year and a time scale for application (refer to information on line)

#### ***Premises License – Regular Events***

Licensed activities include:

- Selling alcohol
- Serving hot food and drink between 11pm and 5am

A premises license is also required for the following types of events, such as:

- Theatrical performances
- Showing a film
- Indoor Sporting Events
- Live Music

- Recorded Music
- Facilities for making Music

A designated premises supervisor is required to be appointed when you apply for a licence, and the license must be displayed.

***Personal Licence – held by the relevant person responsible for authorising the sale of alcohol***

A holder of a Personal Licence is required if you sell alcohol for licensed premises. The holder must be 18 Years + and hold a licensing qualification eg Award for Personal License Holders (APLU) level 2.

**Software Licensing:**

Academies need to ensure that any computer software that may be used on any Academy owned device is appropriately licenced. It is recommended that Academies keep the details of software agreements alongside the hardware inventory to ensure compliance. Further information and guidance can be obtained from Elevate's Premises Manager. Although the nature of software licensing can be complex, license agreements can be categorised into the following areas:

***Operating System Software*** - Microsoft software, which includes Windows, Office and Office 365 are proprietary products from Microsoft and must be appropriately licensed. Apple software, which includes OS X and iOS are products exclusively found on Apple hardware and are usually inclusive with the hardware purchase.

Microsoft offer the following methods for licensing their software:

- Volume License agreement – an agreement to license the whole organisation is provided, which will cover any computer within the purchasing organisation. Agreements are usually calculated on the Full Time Equivalent (FTE) number of staff at the school. This only includes those staff who may use a computer during their duties, so can exclude cleaning teams, midday supervisors etc...
- Open Value (Select) agreements – software licenses are individually purchased and 'allocated' to a user or computer. Organisations who license in this matter should ensure accurate records and an appropriate number of licenses.
- Original Equipment Manufacturer (OEM) – Software is included as part of the hardware purchased and is usually pre-installed. *It is important to note that this software is permanently tied to the hardware purchased, and in the case of replacement or hardware retirement the license is not transferrable and therefore must be purchased again.*

***Third Party software agreements*** - Software developed by third party companies in most cases license their software in one of the following ways:

- Site license – the software is permitted to be used across the purchasing organisation. This is usually a single annual subscription or is calculated on the pupil numbers at the school.
- Physical or virtual 'copy' – A number of licenses are purchased, which are in the form of a physical medium or a license key with a certain number of activations.
- Concurrent license – the license is purchased at a set number of users, which allows the installation of software across the organisation, however the software may only be used up to the license count at any one time.

***Software License Compliance***

It is important to consider the software licenses required when purchasing or consolidating IT hardware. End User License Agreements (EULA) commonly found at the start of software packages are legally binding agreements between the institution and the software company. Academies should refer to their technical support personnel to ensure compliance and record keeping in this area. The school are ultimately responsible for ensuring their software is appropriately licensed.

## Appendix 1:

**Personal Data Breach Procedure:** As set out in the Data Protection policy.

**Actions to minimise the impact of data breaches:** Elevate and their Academies will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. Elevate will review the effectiveness of these actions and amend them as necessary after any data breach.

For data breaches involving disclosure of sensitive information by email we will adopt the following procedure:

**Sensitive information being disclosed via email (including safeguarding records):**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error;
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error;
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask ICT support to recall it;
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way;
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request;
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

**Appendix 2:**

**INFORMATION SECURITY INCIDENT REPORT**

To be completed by the person reporting incident.

**Incident report**

Name of Academy:

Date of incident:

Place of incident:

Name of person reporting incident:

Contact details: email; telephone/address:

Brief description of incident or details of the **personal** information lost including:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned

Brief description of any action taken at the time of discovery **or to be taken including recovery to deal with the breach and to mitigate any possible adverse effects on the individual(s) concerned.**

### Appendix 3:

#### INVESTIGATION

##### Assessing the risks and actions to be taken:

The Compliance Officer will liaise with the Premises Manager and Head teacher to consider the following risk factors when assessing, managing and investigating the incident. This list is not intended to be prescriptive and other relevant factors and issues should be recorded as necessary

##### Incident summary

Summary of the actual or suspected security breach:

--

Date of incident:

Academies / services affected:

People involved in/affected by the incident, (such as staff members, children, contractors, external clients)

Does the incident need to be reported immediately to the police? YES/NO

##### Risk Factor Details and action required

Which IT systems, equipment or devices are involved in the security breach? What information has been lost or compromised?	
How much information has been lost? Is the information unique?	
If the incident involves the loss of a laptop or portable device how recently was the information it held backed up onto central IT systems?	

How important is the information or system to the Academy/Elevate?	
Is it business-critical? Do users rely on access to this particular information asset or can they use reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable?	
How urgently would access need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service?	
Will the loss or compromise of the information have adverse operational, research, financial legal, liability or reputational consequences for the Academy/Elevate or third parties?	
Is the information bound by any contractual security arrangements?	
<p>Is any of the information confidential? Please provide details of any types of information that fall into any of the following Special Categories of data:</p> <ul style="list-style-type: none"> <li>• race</li> <li>• ethnic origin</li> <li>• politics</li> <li>• religion</li> <li>• trade union membership</li> <li>• genetics</li> <li>• biometrics (where used for ID purposes)</li> <li>• health</li> <li>• sex life; or sexual orientation.</li> </ul>	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas.	

Personal information relating to vulnerable adults and children.	
Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed.	
Spread sheets of marks or grades obtained by students, information about individual cases of student discipline.	
Sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	
Any other personal information that would cause damage or distress to individuals if disclosed without their consent Other categories of "high risk" Information.	
Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners Information that would substantially prejudice the Trust or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed.	
Information that would compromise the security of buildings, equipment or assets if disclosed.	
<b>Who else needs to be informed</b>	
Reported to Police?	YES/NO If YES notified on Incident ref:
Major risks escalated to Audit & Resources Committee and Risk Management Register	YES/NO If YES: Date
Notification to Information Commissioner's Office	YES/NO If YES notified on [date]

Notification to data subjects	YES/NO If YES notified on [date]
Notification to other <b>relevant third parties who can help mitigate the loss to individuals, for example, insurers, banks or credit card companies</b>	YES/NO If YES notified on

### Reviewing the incident

The Responsible Officers should meet to review the incident, ensure that all appropriate actions have been taken to mitigate its impact of the incident and to identify further action needed to reduce the risk of a future breach of this kind

How and why the incident occurred:
Actions taken to resolve the incident and manage its impact:
Impact of the incident: (Operational, financial, legal, liability, reputational)
Risks of other adverse consequences of the incident: (Operational, financial, legal, liability, reputational)
Any further remedial actions required to mitigate the impact of the breach:
Actions recommended to prevent a repetition of the security breach:

Resource implications or adverse impacts, if any, of these actions: