DATA PROTECTION POLICY

This document is a statement of the aims and principles of Stanchester Academy, for ensuring the confidentiality of sensitive information relating to staff, students, parents and governors.

Introduction

Stanchester Academy needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Stanchester Academy must comply with the Data Protection Principles which are set out in the Data Protection Act (amended 2003). This policy should also be read in conjunction with the DfE document "Academies and freedom of information" January 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/294920/Academies_and_freedom_of_information_FINAL.pdf

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Stanchester Academy and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Academy has developed this Data Protection Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Academy from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings. It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy. This policy continues to apply to employees and individuals, even after their relationships with the Academy ends.

The Data Controller and the Designated Data Controllers

The Academy as a corporate body is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The Academy has three Designated Data Controllers: They are the Principal, HR Manager and Data & Assessment Manager.
Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the Academy in connection with their employment is accurate and up to date.
- Informing the Academy of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Academy cannot be held responsible for any errors unless the staff member has informed the Academy of such changes.

If and when, as part of their responsibilities, staff collect information about other people(e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Academy staff handbook.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a memory stick or other removable storage media, that media must itself be encrypted or password protected

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the Academy holds and processes about them or their child and
- Why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the Academy is doing to comply with its obligations under the 1998 Act.

To address the first point, the Academy will, upon request, provide all staff and parents **(and students when requested)** and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Academy holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the *Subject Access Request* Form and submit it to the Designated Data Controller.

The Academy will make a **maximum** charge of £10 **(Please refer to appendix B)** on each occasion that access is requested, although the Academy has discretion to waive this **under certain circumstances (e.g. if a parent requests information about their child regarding their education).** The Academy will require that proof of ID is shown upon request.

The Academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, **although good practice recommends 15 working days, as** required by the 1998 Act.

Photographs

Photographs taken at school or during school business are to be used by the school or third parties, under agreement by the school, and do not fall under the DPA as long as they are not for personal use. The school will notify students/parents/carers where this is likely to happen where a notice period is known, but publicity will be generated in all school activities.

CCTV

CCTV is used in schools for the safety and security of students and staff as well as security of the school buildings and contents. The images are not stored permanently on the school site but for a period of 12 hours in the recording device and are never shared with third parties unless a formal request is made as laid out in this policy. A charge for the recording will be made – levied at the cost of producing the recording. Please refer to the Academy's CCTV policy.

Subject Consent

In many cases, the Academy can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the Academy processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The Academy has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The Academy has a duty of care to all staff and students and must therefore make sure that employees and those who use Academy facilities do not pose a threat or danger to other users. The Academy may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The Academy will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the Academy is a safe place for everyone, or to operate other Academy policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered **sensitive** under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the Academy to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of Academy Information

Certain items of information relating to Academy staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the Academy.

Retention of Data

The Academy has a duty to retain some staff and student personal data for a period of time following their departure from the Academy, mainly for legal reasons, but also for other purposes such as being

able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Social Networking

Introduction

New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for schools' staff in many ways. This section sets out Stanchester Academy's protocols on social networking and aims to:

- Assist schools' staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Prevent adults abusing or misusing their position of trust

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in school will always advise the Principal of the justification for any such action already taken or proposed. The Principal will in turn seek advice from the Schools' HR team where appropriate.

This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix C.

Scope

This document applies to all adults who work in Stanchester Academy as adopted by the governing body. This includes teachers, support staff, supply staff, governors, contractors and volunteers.

It should be followed by any adult whose work brings them into contact with pupils. References to adults should be taken to apply to all the above groups of people in schools. Reference to pupils means all pupils at the school including those over the age of 16.
This policy should not be used to address issues where other policies and procedures exist to deal with them. For example any alleged misconduct which falls within the scope of the management of allegations policy requires the school to comply with additional child protection requirements as set out in that policy.

Status

This does not replace or take priority over advice given by Children's Services HR, the school's codes of conduct, dealing with allegations of abuse, other policies issued around safeguarding or IT issues (email, ICT and data protection policies), but is intended to both supplement and complement any such documents.

Principles

- Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults in schools should work and be seen to work, in an open and transparent way.
- Adults in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Safer Social Media Practice in Schools

What is social media?

For the purpose of this policy, social media is the term commonly used for **ALL** websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook and Google+ are perhaps the most well-known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter, snap chat, parlour, et al. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.
For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

Overview and expectations

All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

The guidance contained in this policy is an attempt to identify what behaviours are expected of adults within the school setting who work with or have contact with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

Adults within the school setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

Safer online behaviour

Managing personal information effectively makes it far less likely that information will be misused
In their own interests, adults within school settings need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and

appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

Adults should never make a 'friend' of a pupil at the school where they are working on their social networking page, and should be cautious about becoming 'friends' with ex-students where sibling continue to attend the school.

Staff should never use or access social networking pages of pupils and should never accept an invitation to invite a pupil to become a 'friend'.

Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or the Local Authority could result in formal action being taken against them (refer to staff conduct and disciplinary policies).

Adults are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or the Local Authority into disrepute or could reflect negatively on their professionalism.

Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher/teaching assistant, you should **not** put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the Local Authority.

Protection of personal information

Adults working in schools should:

- Never share their work log-ins or passwords with other people.
- Keep their personal phone numbers private
- Not give their personal e-mail addresses to pupils or parents. Where there is a need for home learning to be sent electronically the school e-mail address should be used.
- Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.
- Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

Adults working in schools should ***not*:**

- Use school ICT equipment for personal use, e.g. camera or computers.

- Use their own mobile phones or home phone to contact pupils or parents – unless there are agreed CP overrides to this*.

Communication between pupils / adults working in school

Communication between pupils and adults by whatever method, should take place within clear and explicit professional boundaries.

This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

**The school normally provides a work mobile and e-mail address for communication between staff and pupils where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers or personal e-mail addresses to pupils or parents for these purposes.*

Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.
Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

Adults should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

There must be awareness on the part of those working with or in contact with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the adult's own family.

Access to inappropriate images and internet usage

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the disciplinary action being taken.

Adults should not use equipment belonging to their school/service to access any adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools need to ensure that internet equipment used by pupils have the appropriate controls with regards to access e.g. personal passwords should be kept confidential.

Where indecent images of children are found, the police and local authority designated officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against adults' policy and should not attempt to investigate the matter or evaluate the

material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution. Refer to the child protection policy for agreed protocols.

Section 3: Link with other policies

This document should be read in conjunction with the following school/ documents:

- School E-Safety Policy
- Disciplinary policy and procedures
- Equal opportunity policy
- CCTV policy
- Code of conduct
- Guidance for Safer Working Practice for Adults who Work with Children and Young People

All adults must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the Academy. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution

Appendix A
Request for Personal Data
under the Data Protection Act

Please complete sections A-C, and return this form together with your fee and proof of identity to the HR Manager, Stanchester Academy (see Section C for details).

A. Your Details

Surname:	Forename:
Former surname(s) (where relevant):	
Postal address: Post code:	Country:
Daytime telephone:	Email:
Date of birth (for identification purposes only):	
Please indicate your relationship with Stanchester Academy: ☐ Current student ☐ Current staff ☐ Other (please specify below): ☐ Former student ☐ Former staff	
If current/former student or staff member, please give subject(s) and dates:	

B. Data Requested

Please describe the data which you are seeking as precisely as you can. Continue on a separate sheet if necessary.

C. Signature

I certify that I am the person named on this form and that I wish to be provided with the data which I have specified relating to myself under the Data Protection Act 1998. I will not publish any data which is supplied to me without prior permission from Stanchester Academy of the copyright owner (if copyright is not owned by Stanchester Academy) except where permitted by law.

Signature: Date:

Please enclose the following with this form:

1. A cheque or money order for £10.00 payable to Stanchester Academy.
2. Proof of your identity. Please supply a photocopy (not originals) of one of the following (if you cannot supply any of these items, please contact Stanchester Academy):

- Your current staff ID (or birth certificate if you are a current or former student)
- The pages which identify you in your passport
- Your driver's licence

Please send your form, fee and proof of identity to:

Stanchester Academy
East Stoke
Stoke sub Hamdon
Somerset
TA14 6UG

Further information about how your request will be handled is available on the Stanchester Academy website www.stanchester-academy.co.uk

D. Data Protection Declaration

The data gathered by this form will be used to process your request for personal data under the Data Protection Act. It will be held by the Data Controller and may be transferred to other parts of Stanchester Academy for the purposes of verifying your identity or processing your request for data. The data will be held for six years from the date when we responded to your request, unless your request forms part of an on-going case, in which case the data will be kept for as long as necessary.

Staff use only

☐ Form received Date:
☐ Fee received Date:
☐ ID received Date:
☐ Response sent Date:

Appendix B
Charges for reproducing data documents

Below is a table of potential charges (if applicable) for copying data documents in school. The exact charge will be communicated to you prior to the commencement of the copying.

Number of pages	Maximum fee
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-69	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

Appendix C
Relevant legislation

School staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

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 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 personal 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 help line staff.
• The school 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.

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 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 new grooming offence 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) and you arrange 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 any 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. Children, Families and Education Directorate page 38 April 2007.
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 school context, human rights to be aware of include:

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

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