Stanchester Academy

Confidentiality Policy 2023-24

Signature: 

Headteacher

Approval Date: July 2023

Review Date: July 2024

Stanchester Academy believes that the safety, wellbeing and protection of our students are paramount. Schools and teachers have access to a plethora of information on each student, held on school databases. It is therefore vitally important that all staff follow the guidelines set out in the various policies and this document highlights the relevant sections from the following three policies: 'E-safety Policy Staff AUP', 'Working at Stanchester Academy (including Code of Conduct)' and 'Data protection policy'.

E-safety Policy Staff AUP

Email

Here are a summary of guidelines for the use of email. Staff should:

- Use caution when sending confidential information in an email as its confidentiality cannot be guaranteed. Messages sent to the wrong address could be used inappropriately and the receiver could save the information indefinitely. Personal, sensitive or confidential information relating to an identifiable individual is subject to the Data Protection Act 1998 and should not be sent by email. Personal, sensitive or confidential information should only be sent via email if the information is contained in a password protected attachment. The password to access the attachment should be verbally communicated to the recipient or sent in a separate email. Personal, sensitive or confidential information should never be included in the main body of an email.

Unacceptable use

Staff should ensure that they do not:

- include any personal, sensitive or confidential information in the main body of an email. For a student this would include their SEND or LAC status, medical information relating to them, child protection issues relating to them, their religious beliefs or political opinions, their physical or mental health issues or their sexual orientation. This would also include more logistical items such as addresses, phone numbers or dates of birth.

Data Protection in the classroom

It is the responsibility of all staff to take care when using, handling or transferring personal data, and as such, all staff will regularly receive support and guidance on Data Protection in briefings and newsletters. Staff must also ensure that they have read the school's "Data Protection Policy" on the website. In and around the classroom, staff should take particular care:

- Not to leave any paperwork containing any sensitive personal data (e.g. Teaching and Learning data sheets including SEN status or Pupil Premium status) in view of students.
- Confidential waste bins are available in Reception. Any confidential documents must be securely deposited in these bins, ready to be destroyed and shredded.
- Not to display SIMs on a whiteboard using a projector, or an interactive whiteboard, even for the taking of registers. The blank/freeze function should be used on AV Projectors/Screens to prevent this.
- At the end of each academic year, teachers should dispose of any paper work containing personal or sensitive information (e.g. teacher planners, mark books, seating plans, student SEND profiles etc.) via the white "confidential waste" bags for shredding. They should also check the "Staff Share" and their personal area of the

network and delete any documents containing personal and sensitive information that will not be needed the following academic year or has been recorded on other systems (e.g. SIMs, 4 matrix, etc.).

Encrypted laptops/USB sticks/hard drives

All staff devices must be encrypted. If for any reason, existing staff realise that their laptop/device is not encrypted, they must contact the IT technical support department immediately. Staff are encouraged to use the school server for document storage and access as this is backed up on a regular basis. Staff must only use their secure encrypted memory stick to transfer day to day files used for teaching and learning purposes, for files that are too large for email attachments, large media/video files or presentations etc. Confidential information like SEND or pupil premium lists should not be stored on encrypted USB sticks or removed from site. Any staff needing advice on how to transfer files should contact the IT technical support department.

Working at Stanchester Academy (including Code of Conduct) Confidentiality

- You may sometimes acquire information at work which has not been made public or is confidential. Examples include information about a student or family, a colleague, information on tenders or costs, the proceedings of confidential meetings.
- You must ensure that sensitive and/or confidential information is properly secured and safeguarded at all times especially if being transported in paper or electronic formats. Particular care must be taken with information stored on portable electronic media such as laptops and memory devices which are often targeted for theft due to their high intrinsic value.
- Confidential Information which comes into your possession must not be used for personal benefit or divulged to other parties except in the proper course of duty, for example to other professionals working with the same child. If you have any doubt whether or not disclosure is appropriate, you must check with the headteacher or line manager before releasing confidential information.
- Some information can be extremely valuable in business and commerce and its publication loss or misuse could seriously disadvantage the school and its employees. Therefore, it is important that you do not, deliberately or inadvertently, pass on information, including software, during or after your employment with the school, to anyone who has no right to receive it. You must not discuss, disclose, publicise or use such information for your own or anyone else's personal interest or advantage.
- You must decline any approaches or offers made asking for information which could be detrimental to, or help others to gain a contract, grant or any other advantage from the school and/or its employees, e.g. a potential contractor could offer a financial reward for information leading to the award of a major contract. Approaches or offers of this kind must be declared to the headteacher without delay.
- You must not criticise the school, its policies or staff in open media such as internet 'blogs', websites, social networking sites, etc. where it may be seen by parents, students or others in the community.

Information technology, social media and data protection

Everyone using computing equipment has a duty of care to use it according to prescribed arrangements, e.g. to avoid introducing computer viruses, to comply with the Data Protection

Act, and to safeguard and ensure the security of information. You must familiarise yourself with the school's IT policies, including use of the internet. In particular, all use of the internet and email facilities must be authorised, legal, appropriate and in accordance with the provisions of the school's policies. Personal use of any facilities – including laptops – must be authorised and only undertaken at times deemed appropriate by the headteacher.

Users shall not use the internet or email for the following:

- to knowingly break the law
- to fail to comply with existing school policy
- to compromise the integrity of any network of system
- to access, display or transmit any kind of sexually explicit material or any offensive or discriminatory material of any kind
- to make unauthorised contact with outside bodies
- to download software or play games
- to bet or gamble
- to disclose private or confidential information

Failure to comply with the policies in force or any unauthorised use of such facilities will be dealt with in accordance with relevant disciplinary procedure.

Data protection policy Data security

- All staff are responsible for ensuring that any personal information, which they hold, or for which they are responsible, is kept securely. This could include information about a variety of members of the school community- including students, staff and parents/carers- e.g. legal guardianship issues, disciplinary records, progress records, reports, references, employment history, taxation and national insurance records, or appraisal records. Staff are also responsible for taking particular care when handling “sensitive personal data”- for a student this would include if they had special educational needs or if they were a “looked after child”, medical information relating to them, child protection issues relating to them, their religious beliefs or political opinions, their physical or mental health issues or their sexual orientation. This would also include more logistical items such as addresses, phone numbers or dates of birth.
- Personal information stored in electronic form must be protected.
- Computers, laptops, tablets, mobile phones and other personal devices used to store or access personal information must be locked whenever they are left unattended.
- Computers, laptops, tablets, mobile phones and other personal devices used to store or access personal information must be password protected. Please refer to the ‘Security’ section of the ‘E-safety Policy Staff AUP’
- Personal information must be kept on the network storage facilities provided
- Personal information that is collected or processed over the internet must only be accessed via a secure encrypted connection using username authentication to prevent unauthorised disclosure
- Personal information must not be transferred via email.
- Personal information must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- All staff must abide by the rules laid out in the “E-safety Policy Staff AUP”, including the “Data Protection in the classroom” section of this.

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated, or otherwise disintegrated for data. Paper files containing sensitive information should be placed in a white “confidential waste” bags for shredding.