HAMPDEN HOUSE

Confidentiality Policy

Adopted by the Management Committee:

Signed: Date: November 2018

Chair of the Management Committee

Date for review: November 2020

Person responsible for review: Headteacher

1. Introduction

Working in any school involves having access in a variety of ways to information that must be regarded as confidential. Therefore, this policy applies to **all** staff employed by the school, including temporary, voluntary and agency staff. It also applies to members of the Management Committee, volunteers and visitors.

This policy must be read in conjunction with the Data Protection (GDPR) Policy, Safeguarding and Child Protection Policy, Staff Disciplinary and Grievance Procedure and the Online Safety Policy.

2. Types of confidential information

Information that is regarded as confidential can relate to:

A range of people, for example:

- students
- parents
- staff/colleagues
- Management Committee members
- job applicants

A range of information, for example:

- home addresses and telephone numbers
- information relating to students' gender, ethnicity, faith, age, special needs, eligibility for student premium, medical conditions
- staff conduct and performance
- staff appraisal and supervision
- staff health/medical
- pay and contracts
- references
- internal minutes and memos
- budgetary information
- other personal information
- unpublished Ofsted reports and judgements

These lists are not exhaustive but will extend to cover any other information of a sensitive nature relating to employees, students and others connected with the school and to the work of the school itself.

3. Potential recipients of information

In the course of daily operation information relating to the school, or those connected with the school, may be requested by, or supplied by, or passed to a range of people.

This might include:

- internal colleagues (teachers, support and residential staff, Senior Leaders)
- colleagues in other schools

- students
- members of the Management Committee
- trade unions/professional associations
- parents/carers
- partner organisations (LA, DfE, Teachers' Pensions)
- other external organisations
- the public
- the press
- contractors/potential contractors

This policy must be adhered to when sharing information with or receiving information from any outside body, agency or individual, with due regard to the Data Protection (GDPR) Policy.

Particular responsibilities

- If someone requesting information is not known to staff, particularly in the case of telephone calls, his/her identity and the legitimacy of his/her request should be verified by calling them back. A person with genuine reasons for seeking information should not object to this precaution.
- Wherever possible, a response to requests for information should only be given when the request has been made in writing.
- The same principle applies when sending emails and faxes. Staff should always check that the information is going to the correct person and is marked confidential where appropriate.
- Being known as an employee of the school may mean being asked for information, for example, by parents/carers about a member of staff who is off sick, or the contact details of another child's parent/carer. Although this can be awkward, parents must be informed that employees are unable to discuss confidential matters or pass on other people's information.
- Persistent enquiries should be referred to the Headteacher.
- The Data Protection Act refers to the principle of third party confidentiality. Information relating to, or provided by, a third party should not be released without the written consent of the third party or unless an order for disclosure is made by a court of competent jurisdiction.

When unsure what to do, staff should refer the matter to the Headteacher for guidance.

4. <u>The form confidential information can take</u>

Confidential information can take various forms and be held and transmitted in a variety of ways. For example:

- manual records (files, teachers' planners, student profiles, Individual Education Plans, attainment data)
- computerised records, CD-ROM and memory sticks
- written reports, minutes, agendas, file notes
- letters, memos, messages
- telephone calls
- face-to-face conversation

- fax
- email
- online
- via the school ICT network

The methods of acquiring information can also vary. Individuals and groups may become aware of confidential information in the following ways:

- access is gained as part of the employee's day to day work
- information is supplied openly by an external third party
- employees may inadvertently become aware of information
- information may be disclosed

Particular responsibilities

Employees should be aware that they may have disclosed to them sensitive information in the course of their work or outside. In some circumstances the individual may request that the information remains confidential.

Staff must be aware that they may be obliged to disclose certain information, for example relating to child protection issues. They must make it clear to the individual disclosing the information that confidentiality cannot be guaranteed and that the information may have to be passed on to someone who can secure the right help, such as the Designated Safeguarding Lead (DSL).

Staff in receipt of confidential information that gives rise to a child protection / safeguarding concern should follow our clear procedures:

- Inform the Designated Safeguarding Lead (DSL) or one of the Alternate DSLs verbally as a matter of priority.
- Confirm this report with a completed handwritten Cause for Concern form.
- If the DSL or Alternate are not available to receive the form it should be posted in the locked Safeguarding Referrals box in the office. An email should be sent to the DSL and alternates to advise them of this.
- If the information appears not to be urgent but might add to a growing picture about a child, the above procedure should still be followed.

Employees should use their discretion regarding these matters, pay due regard to appropriate policies and procedures and, if in doubt, should seek advice from the Headteacher or DSL.

5. Responsibility of individuals in possession of sensitive information

All information received in the course of employment, no matter how it is received, should be regarded as sensitive and confidential. While it is often necessary to share such information, in doing so, employees should consider the following key points.

1. The nature of the information:

- how sensitive is it?
- how did it come to your attention?

2. The appropriate audience:

- who does the information need to be shared with?
- for what purpose?
- who is the information being copied to? Why?
- does restriction of access need to be passed on to your audience?

3. The most appropriate method of communication:

- verbal;
- written;
- email;
- in person.

4. The potential consequences of inappropriate communication.

It is also an individual employee's responsibility to safeguard sensitive information in their possession.

Particular responsibilities

1. Sensitive information should be treated with due respect to the people it concerns.

   Employees at Hampden House are often aware of personal information concerning students and their families. This should only be shared with the relevant personnel, and if not to do so could create barriers or difficulties in supporting the student in question. Under no circumstances should students' personal information become the subject for casual conversation.

2. Sensitive information should be kept secure.

- Filing cabinets should be kept locked when unattended.
- Child protection information is kept in a separate, secure filing cabinet.
- Confidential information should not be left on desks or the photocopier/fax/printer, but should be stored in a locked cabinet, cupboard or drawer, in a room that can only be accessed by authorised personnel.
- Papers should not be left lying around at home or in the car. If confidential materials or paperwork are taken out of the office, precautions must be taken to ensure that they are not accessible to third parties.
- Appropriate steps should be taken to keep track of files which are on loan or being worked on i.e. a record of the date sent and the recipient's name and position.
- If it is necessary to supply confidential files through the external mail, this must be sent by recorded delivery.
- Copies of faxes and emails should be stored securely.

- Steps should be taken to ensure that private and confidential telephone conversations are not overheard.
- Meetings where sensitive or confidential information is being discussed should be held in a secure environment.
- Confidential paperwork should be disposed of correctly either by shredding it or using the confidential waste bin in the school office.
- Personal data should not be used for training or demonstration purposes where fictitious data can be used.

3. Computer data should not be left exposed to others' view when unattended.

- Screen savers should be used when computers are unattended.
- Machines should be switched off over night.
- Unattended computers should be locked.

4. Computer files should be kept securely.

- Passwords should be used and these should not be disclosed to colleagues unless absolutely necessary.
- Staff should not save passwords on their computers in order to log in automatically, but should enter their passwords manually.
- Passwords should be changed periodically (at least every 6 months).
- Sensitive data should not be stored on public folders.
- Staff should be familiar with the security of email/internet systems.
- Staff should use the school email service for all school related emails
- Access to individuals' computers should be restricted.
- Any User IDs and passwords used for the internet should remain confidential.
- All work carried out on a computer should be stored safely either in a personal directory, or onto a memory stick or portable hard drive which should be kept securely.
- Computer files should backed up regularly and not solely saved to the hard disk.

5. A variety of phrases may be used on correspondence to denote confidentiality. As a general rule:

- Post marked 'personal' or 'for the attention of the addressee only' should only be opened by the addressee personally;
- Post marked 'private' and/or 'confidential' may be opened by those responsible for distributing the post within the school.

6. Confidential mail which is then forwarded internally should continue to carry a confidential tag.

6. Other responsibilities

Employees should have regard to potential difficulties which may arise as a result of discussions outside work. While it is natural (and indeed can be therapeutic) to talk about work at home or socially, staff should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on. Staff should be particularly aware that many people have a direct interest in education and schools and even close friends may inadvertently use information gleaned through casual discussion.

Personal and work-related information relating to individuals, should not be disclosed to third parties except where the individual has given their express permission or where this is necessary to the particular work being undertaken.

The Headteacher should comply with the procedures for the storage and sharing of information relating to individuals' Appraisal Reviews.

Personal and case files should not normally be shared with third parties other than those responsible for writing references. Exceptions may apply in the case of legal proceedings.

Employees should use their discretion in these matters and if in doubt, should seek advice from the Headteacher.

7. The consequences of revealing confidential information without authority

Staff should ensure that they are familiar with this Confidentiality Policy and related policies. While there is an expectation that staff will use their professional discretion in applying the policy, they should always seek advice when they are unsure.

Staff should be aware that serious breaches of the policy may result in disciplinary action being taken. The severity of the sanction will be assessed with regard to the potential harm the disclosure will have caused to the individual concerned. Some breaches of confidentiality could be regarded as potential serious or gross misconduct that could result in dismissal.