Trinity High School
& SIXTH FORM CENTRE
An Independent State Funded Academy

DATA PROTECTION POLICY

including

PROCEDURE COVERING MANAGEMENT AND CONTROL OF CCTV SYSTEM

Reviewed:	Sept 2012
Adopted by Governing Body:	11 Dec 2012
Review date:	Sept 2015

DATA PROTECTION POLICY

The Governing Body of Trinity High School adopted this scheme on 11 December 2012.

The School holds and processes information about its staff, applicants, students, parents/carers, and other individuals who come into contact with the School who are defined as 'data subjects' under the Data Protection Act 1998. The School processes personal data for a variety of reasons including to monitor attendance and academic progress, health and safety reasons and other statutory requirements. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

COMPLIANCE WITH THE DATA PROTECTION ACT 1998

The School takes the protection of all personal data very seriously and to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Personal information must be dealt with properly however it is collected, recorded and used, whether on paper or in electronic form.

To this end we fully endorse and adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met ;
2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. Shall be accurate and, where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The School and all staff who process, hold or use any personal information must ensure that they follow these principles at all times.

THE DATA CONTROLLER

The Governing Body is responsible for the implementation of the terms of the Data Protection Act and is responsible for appointing someone with specific responsibilities for data protection within the School. This includes annual registration with the Information Commissioner as required by the Data Protection Act.

The current appointee is **Mr Ward**, Deputy Head.

RESPONSIBILITIES OF STAFF

All staff are responsible for:

- Checking that any information they provide to the School in connection with their employment is accurate and up to date
- Informing the School of any changes to information which they have provided, e.g. changes of address, telephone numbers
- Informing the School of any errors in the information that the School holds about them
- The School cannot be held responsible for any errors of which it has not been informed.

RESPONSIBILITIES OF PARENTS/CARERS

All parents/carers are responsible for:

- Checking that any information they provide to the School is accurate and up to date
- Informing the School of any changes to information which they have provided, e.g. changes of address, telephone numbers
- Informing the School of any errors in the information that the School holds about them

The School cannot be held responsible for any errors of which it has not been informed.

DATA SECURITY

- All staff are responsible for ensuring that any personal information, which they hold, or for which they are responsible, is kept securely
- Personal information stored in electronic form must be password protected
- Computers used to access personal information must be locked whenever they are left unattended
- Personal information must be kept on the network storage facilities provided
- If it is necessary to take personal information off-site, e.g. on a laptop or memory stick, the medium MUST be encrypted and transferred back to the network as soon as possible
- 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 unless it has been encrypted

- Personal information must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

RETENTION OF DATA

The School will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements. Advice on the collection, retention and secure storage of information may be obtained from the Data Controller.

RIGHTS TO ACCESS INFORMATION

All data subjects have the right to access any personal information that is held about them. They also have the right to have inaccurate data corrected, destroyed or erased. Any person who wishes to exercise this right should contact the School's Data Controller in writing. Your letter should include your name and contact details. The School may ask for further information in order to confirm your identity. The School reserves the right to make a charge of up to £10 for each access request. The School will comply with the request within 40 days from the date that the written request is received.

COMPLIANCE

Unauthorised disclosure of personal information is in breach of the Data Protection Act 1998 and may result in disciplinary action. In some cases it may be considered as gross misconduct and may result in a personal liability for the individual staff member.

Any data subject, who feels that this Data Protection Policy has not been correctly followed with regard to personal information about themselves, should raise the matter initially with the Data Controller. If they feel that the matter has not been resolved it should be raised as a formal grievance.

PROCEDURE COVERING MANAGEMENT AND CONTROL OF CCTV SYSTEM

INTRODUCTION

The purpose of the CCTV surveillance system is to protect Trinity High School assets, and provide an additional level of personal security for staff, pupils and visitors.

The system is covered under the terms of the Data Protection Act with Trinity High School as the Data Controller. Tese procedures are intended to support the School's obligations, in respect to the control and management of data processed by the CCTV system.

The CCTV systems installed on the Trinity High School site consists of 8 fixed (Grove Block) and 10 fixed and 6 steerable (Main building) camera positions. The cameras are linked to two main controller and recording facilities located in the General Office and Visitors Reception, with a monitoring facility positioned in both locations. The systems were installed by T&S Solutions and Elgan Technology Ltd and are each covered by a maintenance agreement.

Appropriate signs are in place to warn visitors they are entering a site where CCTV surveillance is in operation.

AUTHORISED USERS

The Deputy Headteacher is responsible for the School's data protection policies, and as such oversees the use of the CCTV system.

Access to the CCTV systems is restricted to authorised persons, as follows:

- Members of the Senior Management Team
- School Site staff, with responsibility for the site after normal school hours
- Staff working in the General Office and Visitors' Reception who are required to work at these stations

All staff comply with the CCTV Code of Practice issued by the Information Commissioners Office (2008). This document is available on the R Drive. External requests for information from the CCTV system are referred to the Deputy Headteacher who keeps appropriate records of all such requests.