



Data Protection Policy

If you think our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer: dpo@davidgamecollege.com

Alternatively, you can make a complaint to the Commissioner's Office.

- Report a concern online at <https://ico.org.uk/concerns>
- Call 0303 123 1113
- Or write to: information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**. The **personal data breach procedure** can be found in appendix 1 of this policy.

AIMS

Our college aims to ensure that all personal data collected about staff, pupils, parents, guardians, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the expected provisions of the GDPR and DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

DEFINITIONS

| Term | Definition |
|--|---|
| Personal data | Any information relating to an identified, or identifiable, individual. This includes the individual's: <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as username |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none">• Ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership• Genetics• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes• Health – physical or mental• Sex life or sexual orientation |
| Processing | Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. |
| Data subject | The identification of, or identifiable, individual whose personal data is held or processed (e.g. all our students, parents or guardians and staff will be data subjects). |
| Data controller | A person or organisation that determines how and why personal data is processed (e.g. college). |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. |

1. INTRODUCTION

David Game College processes personal data relating to employees, students, parents, guardians, visitors and others to allow us to monitor performance e.g. appraisals, achievements, and health and safety, for example, and is therefore a data controller. The College is registered as a **data controller** with the ICO and will renew this registration annually or as otherwise legally required. It is also necessary to process information in order

to recruit and pay staff, organise courses and comply with legal obligations to funding bodies and government. 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, David Game College must comply with the **Data Protection Principles** which are set out in the GDPR and DPA (2018). In summary these state that personal data must be:

- obtained and processed fairly, lawfully and in a transparent manner
- collected for specified, explicit and legitimate purposes and shall not be processed in any manner incompatible with that purpose
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary for the purposes for which it is processed
- processed in a way that ensures it is appropriately secure, kept safe from unlawful or unauthorised access, accidental loss, damage or destruction
- where we transfer data to a country outside the European Economic Area, we will do so in accordance with data protection law

This policy sets out how the College aims to comply with these principles.

2. STATUS OF THE POLICY

- a. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.
- b. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the DPO initially. If the matter is not resolved it should be raised as a formal grievance.

3. DESIGNATED DATA PROTECTION OFFICER

- a. The **data protection officer (DPO)** is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
- b. The DPO will provide an annual report of the activities directly to the principal and, where relevant, report to the principal, vice-principals and IT manager any advice and recommendations on college data protection issues.
- c. The DPO is also the first point of contact for individuals whose data the College processes, and for the ICO.
- d. Full details of the DPO's responsibilities are set out in their job description.
- e. Our DPO is Alexandra Raen and is contactable via dpo@davidgamecollege.com

4. PRINCIPAL AND VICE-PRINCIPALS

The principal and vice-principals act as the representatives of the data controller on a day-to-day basis.

5. IT MANAGER

The IT manager, Zed Abaderash, zed@davidgamecollege.com acts as the representative of the data controller's IT on a day-to-day basis.

6. ALL STAFF

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the College of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to reply on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer data outside the European Economic Area
 - If there has been a data breach
 - Whether they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

7. COLLECTING PERSONAL DATA

7.1 LAWFULNESS FAIRNESS AND TRANSPARANCY

We will only process data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the College can **fulfil a contract** with the individual, or the individual has asked the College to take specific steps before entering into a contract
- The data needs to be processed so that the College can **comply with a legal obligation**
- The data needs to be processed to ensure **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the College, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the College or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or the parent/guardian/carer when appropriate) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing data which are set out in the GDPR and DPA 2018.

For **online services** provided to pupils, such as usernames to access classroom apps and resources, and parents or guardians, such as access to reports and progress data, we intend to rely on consent as a basis for processing from pupils and parents or guardians respectively, and we will obtain parental consent where the pupil is under 13 (except for online counselling and preventative

services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 LIMITATION, MINIMISATION AND ACCURACY

We will only process data for **specified, explicit** and **legitimate** reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek **consent** where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the College's **record retention schedule** within the **records management policy** (appendices 3 and 6).

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/guardian that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – e.g. IT companies like SchoolBase (also see our **sensitive data email policy** and **online safety ICT policy** in appendices 4 and 5). When doing this, we will:
 - Only appoint IT suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep data safe while working for us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding, mental health and special educational need (SEN) obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer data to a country outside the European Economic Area, we will do so in accordance with data protection law.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 13 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that staff and those who use the College facility do not pose a threat or danger to other users.

Therefore, all staff and pupils will be asked to sign a **consent to process declaration**, regarding particular types of information, when an offer of employment or a course place is made.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the College holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for an individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 CHILDREN AND SUBJECT ACCESS REQUESTS

Personal data about a pupil belongs to that pupil, and not the pupil's parents, guardians or carers. For parents, guardians or carers to make a subject access request with respect to their child or ward, the child or ward must either be unable to understand their rights and the implications of a subject access request, or have given their **consent**.

Pupils aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents, guardians or carers of pupils at our College may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to requests, we:

- May ask the individual to provide **two forms of identification**
- May contact the individual via phone to conform the request was made
- Will respond without delay and within **one month** of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within **three months** of receipt of the request, where a request is complex and numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the pupil is at risk of abuse, where the disclosure of the information would not be in the pupil's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the pupil

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee of up to £30 which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, guardians or carers, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within **fifteen school days** of receipt of a written request.

All **data subjects** are responsible for:

- Checking that any information that they provide to the College in connection with an individual or themselves is **accurate** and **up-to-date**
- Informing the College of any **changes** to information e.g. changes of address
- **Checking** the details of information kept and processed about individuals that the College will issue to individuals from time to time
- Informing the College of any **errors or changes** – the College cannot be held responsible for any errors unless the **data subject** has informed the College

11. CCTV

We use ICT in various locations around the College premises to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the **IT Manager**.

12. PHOTOGRAPHS AND VIDEOS

As part of our College activities, we may take photographs and record images of individuals within or College.

We will obtain written consent from parents, guardians or carers, and pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent, guardian or carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph or video will be used.

Uses may include:

- Within the College on notice boards and in College magazines, brochures, newsletters, etc.
- Outside of College by external agencies such as the college photographer, newspapers, campaigns
- Online on our College website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the pupil, to ensure they cannot be identified.

As much information on staff is made public as possible, and in particular the following information will be available to the public for inspection:

- Names and means of contacting College senior managers and leaders
- Photographs displayed on notice boards of key staff (e.g. SMT, Safeguarding lead, etc.)

The College's internal phone list will not be a public document.

See our **safeguarding and child protection policy** as well as our **photograph and video policy** on photography for more information on our use of photographs and videos.

13. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appoint a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 1)
- Completing **privacy impact assessments** where the College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on the process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly **conducting reviews and audits** to test our privacy measures and make sure we are compliant
- Maintaining **records** of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our College and DPO and all information we are required to share about how we use and process their personal data (via our privacy policies)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office or classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the College office
- **Passwords** that are at least 8 characters long containing letters, numbers and special characters are used to access College computers, laptops and other electronic devices and removable media, such as laptops and USB drives
- Encryption software is used to protect all portable devices and removable media such as laptops and USB drives

- Staff, pupils or others who store personal information on their personal devices are expected to follow the same security procedures as for College-owned equipment (see our **online safety and ICT policy** on acceptable use and our **acceptable use agreement**)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

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

Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

15. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become **inaccurate** or **out-of-date** will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will **shred** or **incinerate** paper-based records, and overwrite or **delete** electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. PERSONAL DATA BREACHES

The College will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach, to the ICO within **72 hours**. Such breaches in the context of the College may include, but are not limited to:

- A non-anonymised dataset being published on the College website which shows the exam results of pupils
- Safeguarding information being made available to an unauthorised person
- The theft of a College laptop containing non-encrypted personal data about pupils

17. PROCESSING OF SENSITIVE INFORMATION

Sometimes it is necessary to process information about a person's **physical health**, details of **criminal convictions**, **racial or ethnic origin**, **political opinions**, **religious beliefs**, trade union activities, **sexual life**, or details of **mental health**. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or the equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. More information on specific cases about this is available from the data protection officer, your head of department, the personnel department or the student services office.

18. EXAMINATION MARKS

Students will be entitled to information about their marks for both coursework and examination. However, this may take longer than other information to provide.

19. RETENTION OF DATA

A schedule detailing the College data retention can be found in the **Data Retention Schedule** (appendix 6).

20. TRAINING

All staff are provided with data protection training as part of their **induction** process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the College's processes make it necessary.

21. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (DPA 2018 on the 25th May) – if any changes are made to the bill that affect our College's practice. Otherwise, or from then on, this policy will be **reviewed every 2 years** and shared with the full governing body.

22. CONCLUSION

Compliance with the 2018 Act is the **responsibility** of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the data protection officer.

APPENDIX 1. PERSONAL DATA BREACH PROCEDURE

This procedure is based in guidance on personal data breaches produced by ICO.

- On finding or causing a breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered

- Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the principal and vice-principals
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control of their data
 - Discrimination
 - Identity theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on College's network drive in a secure folder
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in a secure College network folder

- The DPO, principal and vice-principals will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

We 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. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Types of breaches may include:

- **SENSITIVE INFORMATION BEING DISCLOSED VIA EMAIL** (including safeguarding, physical and mental health, SEN records, etc.)
- **DETAILS OF PUPIL INTERVENTIONS BEING PUBLISHED ON THE COLLEGE WEBSITE**
- **A COLLEGE LAPTOP OR USB DRIVE CONTAINING NON-ENCRYPTED SENSITIVE PERSONAL DATA BEING STOLEN OR HACKED**
- **THE COLLEGE'S ACCOUNT PAYMENT DEPARTMENT BEING HACKED AND PARENTS' FINANCIAL DETAILS STOLEN**

APPENDIX 2. DISCLOSURES AND DISCLOSURE INFORMATION

General Principles

As an organisation using the Disclosure and Barring Service (DBS) to help assess the suitability of applicants for positions of trust, David Game College complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. It also complies fully with its obligations under the Data Protection Act and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Disclosure information and this is our College statement on these matters.

Storage and Access

Disclosure information is never kept on an applicant's personnel file and is always kept separately and securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling

Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed and we recognise that it is a **criminal offence** to pass this information to anyone who is not entitled to receive it.

Usage

Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

APPENDIX 3. RECORDS MANAGEMENT

Requirement

Background

Section 46 of the Freedom of Information Act 2000 requires colleges and schools to follow a Code of Practice on managing their records. Under section 7 of the Code of Practice on the Management of Records, it states that: "Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy."

[For a full copy of the Lord Chancellor's Code of Practice see [Code of Practice](#)]. The General Data Protection Regulation (GDPR) also does not stipulate how long records should be kept for. It is similar to the Code of Practice, in that personal data must be kept no longer than necessary for the purposes for which it was originally processed. It simply requires all colleges, schools, including independent schools, not to keep records for longer than necessary.

[Contact us, ICO](https://ico.org.uk/global/contact_us) https://ico.org.uk/global/contact_us

Aims

David Game College recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the College, and provide evidence for demonstrating performance and accountability.

Retaining large quantities of information is not necessarily the safest option, as the College is **at risk of a fine** if it cannot show that it is keeping information for the right purposes.

This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

Record retention schedule

A table, see **retention schedule** in appendix 6, shows the retention periods for different types of records, and the actions to take at the end of a record's administrative life. For some records, there are statutory retention periods. For others, the table shows **retention guidelines** following expected best practice.

Managing records using these retention guidelines is considered "normal processing" under the Data Protection Act 1998 and the Freedom of Information Act 2000. Page 35 adds:

"If record series are to be kept for longer or shorter periods of time than laid out in this document the reasons for this need to be documented."

Scope

1. This policy applies to all records created, received or maintained by staff of the College in the course of carrying out its functions.
2. Records are defined as all those documents which facilitate the business carried out by the College and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
3. A small percentage of the College's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

Responsibilities

1. The College has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Principal of the College and the Vice-Principal of the College.
2. The person responsible for records management in the College will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.
3. Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the College's records management guidelines.

Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the College.

Signed: _____ [Principal of David Game College]

Signed: _____ [Vice-Principal of David Game College]

Pupil Records

These guidelines are intended to help provide consistency of practice in the way in which pupil records are managed. These will assist the College about how pupil records should be managed and what kind of information should be included in the file. It is hoped that the guidelines will develop further following suggestions and comments from those members of staff who have the most contact with pupil records. These guidelines apply to information created and stored in both physical and electronic format. These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact the Local Authority.

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every educational institute they attend and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all

information relating to the pupil will be found in the file (although it may spread across more than one file cover).

File covers for pupil records

The pupil record starts its life when a file is opened for each new pupil as they enrol. This is the file which will follow the pupil for the rest of his/her school career.

A consistent file cover for the pupil record must be used. Using a pre-printed file (hard-copy or electronic) ensures all the necessary information is collated and the record looks tidy, and reflects the fact that it is the principal record containing all the information about an individual child.

Pre-printed file covers are not being used then the following information should appear on the front of the paper file:

- Surname
- Forename
- DOB
- Special Educational Needs, Medical Needs Yes/No [This is to enable the files of pupils with special educational needs or medical needs (including physical or mental health) to be easily identified for longer retention]

The file cover should also contain a note of the date when the file was opened and the date when the file is closed.

Inside the front cover the following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin [although this is "sensitive" data under the Data Protection Act 1998, the Department for Education require statistics about ethnicity]
- Language of home (if other than English)
- Religion [although this is "sensitive" data under the Data Protection Act 1998, the College has good reasons for collecting the information]
- Any allergies or other medical conditions that it is important to be aware of [although this is "sensitive" data under the Data Protection Act 1998, the College has good reasons for collecting the information]
- Names of parents and/or guardians with home address and telephone number (and any additional relevant carers and their relationship to the pupil)
- Name of the College, admission number and the date of admission and the date of leaving.
- Any other agency involvement e.g. speech and language therapist, paediatrician
- It is essential that these files, which contain personal information, are managed against the information security guidelines as set out in the **data protection policy**.

Recording information

Pupils have a right of access to their educational record and so do their parents under the Education (Pupil Information) (England) Regulations 2005. Under the Data Protection Act 1998 a pupil or their nominated representative has a right to see information held about them. This right exists until the point that the file is destroyed. Therefore, it is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

Transferring the pupil record to the College

The pupil record should not be weeded before transfer to the secondary school or college unless any records with a short retention period have been placed in the file. It is important to remember that

the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Previous schools or colleges do not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. Custody of and responsibility for the records passes to the college the pupil transfers to, which is David Game College.

Files should not be sent by post unless absolutely necessary. If files are sent by post, they should be sent by registered post with an accompanying list of the files. David Game College should sign a copy of the list to say that they have received the files and return that to the primary school or previous school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

David Game College records

Items which should be included on the pupil record

- If the pupil has attended an early years setting in the UK, then the record of transfer to a primary school should be included on the pupil file
- Admission form (application form)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Years Record
- Annual Written Report to Parents
- National Curriculum and Religious Education Locally Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the pupil
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in a sealed envelope clearly marked as such)
- Child protection reports/disclosures (should be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files once the pupil leaves the College.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

Responsibility for the pupil record once the pupil leaves the College

The College which the pupil attended until statutory school leaving age, the college where the pupil goes on to complete their sixth form studies, is responsible for retaining the **common transfer**

file until the pupil reaches the age of 25 years. [See the **retention schedule** in appendix 6 for further information].

Safe destruction of the pupil record

The pupil record should be disposed of in accordance with the **safe disposal of records** guidelines.

Transfer of a pupil record outside the EU area

If the College is requested to transfer a pupil file outside the EU area because a pupil has moved into that area, we will transfer data to a country outside the European Economic Area, but we will do so in accordance with data protection law.

Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in **lockable storage** areas with **restricted access**, and the contents should be secure within the file. Equally, electronic records should have appropriate **security**. Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

No copies of any records in the pupil's record will be kept, unless there is an ongoing legal action when the pupil leaves the College.

Common transfer file

Our College (where the pupil completes sixth form studies) is responsible for keeping the common transfer file until the pupil reaches the age of 25.

Other types of files

Keeping any other files for "as long as necessary" we take a common sense approach before disposing of them.

Such files could include non-statutory teacher assessment information, minor behavioural notes or information about the pupil's family [see **retention schedule**].

Where possible, any information received from primary schools or previous schools should be uploaded onto the College's information management system during the autumn term.

Staff records

Staff personal files are retained for **six** years following the end of a staff member's employment, before disposing of them securely. Some files may need to be kept for longer, for example if a staff member was involved in any child protection issues, in which case it will be kept for **twenty** years. Records of injury at work or accidents are kept for **twelve** years.

If pensionable information is kept on the personnel file, this will need to be retained until six years after the last pension payment has been made.

Different parts of the personal files of staff who have left the College, have different retention periods [see **retention schedule** table in appendix 6]. Thus gradually removing parts of the file in accordance with their retention periods, so that eventually the file will just contain the employee's start date, end date, tax and pension information and whether or not they were fired.

Storage

The seventh principle of the Data Protection Act states:

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.

It does not define the security measures that an organisation should have in place.

[Data Protection Act 1998: schedule 1, part 1, legislation.gov.uk](http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/1)
<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/1>

The ICO has published an overview of the requirements of this principle.

What kind of security measures might be appropriate?

Measures taken at an organisation-wide level:

- How to ensure that staff are aware of their data protection responsibilities
- The security of premises and paper-based records
- Computer security

[Information security \(principle 7\): What kind of security measures might be appropriate? ICO](http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7#appropriate-measures)
http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7#appropriate-measures

In short, the ICO representative advised that hard copies of records should be safely secured in a lockable filing cabinet, and that **electronic records should be password-encrypted**.

Information Security and Business Continuity Information

Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with the Data Protection Act 1998.

Taking measures to protect our records can ensure that:

- Our college can demonstrate compliance with the law and avoid data loss incidents
- In the event of a major incident, our college should be able to stay open and will at least have access to its key administrative and teaching records. An **information security policy** incorporates a **business continuity plan** and deals with records held in all media across all College systems:
 - Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images)
 - Hard copy (including but not limited to paper files, plans)
- **Digital Information** – In order to mitigate against the loss of electronic information our College needs to:
 - Operate an effective backup system:
 - Undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Where possible these backups are to be stored in a different building to the servers and off the main College site. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible.
 - Use of an off-site, central back up service (usually operated by the local authority or other provider). This involves a backup being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the College.

- Storage in a data safe in another part of the College premises. The backup will be stored in a fireproof safe which is located in another part of the premises. These premises must also be physically secure and any hard copy supporting data regarding the location of records should also be stored in the safe.
 - Control the way data is stored within the College:
Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff should be advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, and portable hard drives, USBs or even on CD.
 - Maintain strict control of passwords:
All staff members ensure that the data is subject to a robust password protection regime, ideally with users changing their passwords every 30 days. Discourage password sharing strongly and seek alternative ways for users to share data – like shared network drives or proxy access to email and calendars. In addition staff should always lock their PCs when they are away from the desk to prevent unauthorised use.
 - Manage the location of server equipment:
We ensure that the server environment is managed to prevent access by unauthorised people.
 - Ensure that business continuity plans are tested:
We test restore processes on a regular basis to ensure that the first time you identify a problem with the backup is not the first time you need to retrieve data from it. For advice on preserving information security when using email see the fact-sheet on **good practice for managing email policy** (see appendix 4).
- **Hard Copy Information and Records** – Records which are not stored on the College’s servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.
 - Fire and flood:
The cost of restoring records damaged by water can be high but a large percentage may be saved, fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all vital information should be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water.
Where possible vital records should not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood. The bottom shelves of a storage cupboard should be raised at least 2 inches from the ground. Physical records should not be stored on the floor.
 - Unauthorised access, theft or loss:
Staff are encouraged not to take personal data on staff or students out of the College unless there is no other alternative. Records held within the College should be in lockable cabinets. Access to offices in which personal information is being worked on or stored is restricted. All archive or records storage areas are lockable and have restricted access.
Where paper files are checked out from a central system, log the location of the file and the borrower, creating an audit trail.
For the best ways of disposing of sensitive, personal information see **safe disposal policy**.
 - Clear Desk Policy:
A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/ or flood damage.

A clear desk policy involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

Disclosure

Staff should be aware of the importance of ensuring that personal information is only disclosed to people who are **entitled to receive** it. Ensure that where you intend to share personal information with a third party that you have considered the requirements of the Data Protection Act. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address which can be verified. You may wish to develop a data sharing protocol with the third parties with whom you regularly share data (e.g. send anonymised data, consent had been signified, justifiable need-to-know purpose).

Indemnity

Each partner organisation and member of staff will keep each of the other partners and staff members fully indemnified against any and all costs, expenses and claims arising out of any breach of the **acceptable use agreement** and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub- contractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with the agreement **acceptable use agreement**.

Risk Analysis

The College will undertake a business risk analysis to identify which records are vital to College management and these records should be stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks.

The development of an information asset/risk register will assist with this process.

Responding to Incidents

In the event of an incident involving the loss of information or records the College should be ready to pull together an incident response team to manage the situation. The specific member of staff to deal with press/media enquiries will be either the principal or vice-principals.

Major Data Loss/Information Security Breach

This process must be used by all members of staff if there is a major data loss or information security breach. The DPO will liaise with the Information Commissioner's Office if an information security breach needs to be reported. The Information Commissioner's Office will be notified immediately if the incident is serious enough to justify notification, for it is better to have notified the Information Commissioner before someone makes a complaint to him.

Fire/Flood Incident

The team of people who are trained to deal with a fire/flood incident will include the janitor, the vice-principals, the IT manager, security staff and fire marshals. This will include the provision of an equipment box, the appropriate protective clothing and an emergency data protection plan. The team, equipment and emergency plan should be reviewed on a regular basis.

Disposal

Who can dispose of physical documents?

Any member of staff dealing with a specific data set can shred or dispose of confidential documents provided the destruction was authorised by the relevant responsible person; any accreditation of the data disposal person would not be required.

Where an external provider is used, all records should be shredded onsite in the presence of an employee. Staff working for the external provider "should have been trained in the handling of confidential documents".

Types of disposal:

- Disposing of records that have reached the end of their minimum retention period
- Transferring records to archives
- Transferring information to other media
- Recording all archiving, destruction and digitisation of records

Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

Disposal of records that have reached the end of their retention period

The fifth data protection principal states: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"

Records that are no longer required for use are to be reviewed as soon as possible so that only the appropriate records are destroyed. This review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained for research or litigation purposes.

Whatever decisions are made, they need to be **documented** as part of the **records management policy** (in appendix 3).

Safe destruction of records

All records containing personal information, or sensitive information should be made either unreadable or unreconstructable:

- Paper records should be shredded using a cross-cutting cutter
- CDs/DVDs/Floppy Disks should be cut into pieces
- Audio/Video Tapes/Fax Rolls should be dismantled and shredded
- Hard Disks/USBs should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Records cannot be put in with the regular waste or skip. The confidential waste bin service could be used.

All destruction of records must be authorised by the relevant responsible person.

Freedom of Information Act 2000 (FoIA 2000)

The Freedom of Information Act 2000 requires the College to maintain a list of records which have been destroyed and who authorised their destruction (these lists of destroyed records could be kept in a spreadsheet or other database format).

- Members of staff should record at least:
- File reference (or unique identifier)
- File title (or brief description)
- Number of files and date range
- Name of the authorising person
- Date action taken

Following these guidelines will ensure the College is compliant with the Data Protection Act 1998 and the Freedom of Information Act 2000.

Transfer of records to the archives

Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service. The College should contact the local record officer if there is a requirement to permanently archive the records, and the records will continue to be managed via the **DPA 1998** and the **FoIA 2000**.

If you would like to retain archive records in a special archive room in the College for use with pupils and parents, please contact the local record office for specialist advice.

Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of media and the ability to migrate data where necessary should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to follow the procedures so that conversion is done in a standard way. This means the College can prove that the electronic version is a genuine original and could not have been tampered with in any way. If someone were to query an electronic record, our College may be in a better position to confirm the accuracy of the electronic record if we were able to back it up with the original hard copy.

Transfer to media procedure

For members of staff who are required to write (copy/move) data to removable media (memory stick, or CD/DVD):

- All removable or portable storage devices used for data transfer must be encrypted
- Encrypted portable storage devices must be password protected with a strong password and kept secure for future retrieval
- The transferor must check at an appropriate time that the transfer has been successful and make an entry on a converted-to-electronic-media spreadsheet. Report any issues to the person in charge and in the case of missing or corrupt data to the DPO immediately.

Electronic records

The owner of electronic records will need to state the purpose and statutory requirements for keeping the records as well as the retention period.

This statement should also contain the named person responsible for long-term data preservation. This statement should be updated whenever there is a restructure which changes the person responsible or the format or location of the stored data.

A brief description of the supported file formats, software specification/licence information for long-term preservation (e.g. Word or PDF) should also be included. If this information is not retained, it is possible that the data contained electronically may become inaccessible as a result and unusable with all of the ensuing consequences.

Long-term preserved data must be accessible when required but must also be protected against the standard information security requirements. It must be stored in a way that does not cause a health and safety hazard. Records must not be stored in corridors and must not impede or block fire exits. There should be appropriate heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area should be secured against intruders and have controlled access. If it is an office, it should be locked at all times while the responsible person is not in the office. These storage areas should be regularly monitored and checked for any damage or emergency risks, especially during the holiday periods.

Hazards

The following are hazards which need to be considered before approving areas where physical or electronic records can be stored:

- Fire damage:

Records (paper or electronic) can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although fire and water damage can usually be repaired.

Records should be kept in fire resistant cabinets. Metal filing cabinets will usually suffice, but for important core records, fire proof cabinets may need to be considered, as they are expensive and very heavy, careful consideration is needed to identify crucial core data.

Records kept in cupboards or in desks will suffer more damage than those stored in a filing cabinet.

- Water damage:

Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive; therefore, records need to be protected against water damage where possible. Records should be stored at least 2 inches off the ground. Storage boxes and portable storage containers should be raised by at least 2 inches off the ground. This is to ensure that in the case of a flood records are protected against immediate flood damage. Electronic data can also be damaged in water, therefore the same principles apply. Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

- Sunlight damage:

Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade, dry out and become brittle or electronic media to be damaged or corrupted.

- Humidity damage:

Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records, or damage electronic media. Mould can be a hazard to human health and will often damage records beyond repair.

Temperature range should not exceed 18°C and the relative humidity should be between 45% and 65%.

Temperature and humidity should be regularly monitored and recorded. Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

- Insect/rodent damage:

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice).

College closure and record keeping

If the College has been closed and the site is being sold or reallocated to another use, the local authority (LA) should take responsibility for the records from the date the College closes.

If two colleges have merged and function as one, it will be necessary for the new College to retain any records originating from the two colleges "for the appropriate time".

When a college closes records management is often low on the list of priorities. Closures are often imposed on colleges or schools, therefore, at the time where records management needs to be considered the staff at the College will be on different parts of the change management cycle.

The College will have records which will need to be assessed and either:

- Securely disposed of
- Stored securely until the end of the statutory retention period
- Transferred to another organisation (for example the LA)
- Transferred to the appropriate County Record Office

Sufficient time to ensure that the records have been properly sorted, listed and boxed before transfer to the LA must be allowed as part of the project timescales of the College closure. Proper resources must be allocated to ensure that the job can be completed before the College closes.

APPENDIX 4. MANAGING EMAIL GOOD PRACTICE

Introduction

These guidelines are intended to assist David Game College staff to manage their email in the expected and most effective way, and must be used in conjunction with our College's policies on the use of the **online safety ICT policy**. Information about how-your-email-application-works is not included in this document.

Eight things you need to know about email

Email has replaced telephone calls and memos

As communicating by email is quick and easy, many people have replaced telephone conversations and memos with email discussions. However, the language in which email is written is often less formal and more open to misinterpretation than a written memo or a formal letter.

Remember that email should be laid out and formulated to our college's standards for written communications.

Email is not always a secure medium to send confidential information

You need to think about information security when you send confidential information by email. The consequences of an email containing sensitive information being sent to an unauthorised person could be a civil penalty of up to £500,000 from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a **secure encrypted email** system.

Never put personal information (such as a pupil's name) in the **subject line** of an email.

Email is disclosable under the access to information regimes

All College email is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public, so too if you use a personal email address for official correspondence.

Email is not necessarily deleted immediately

Emails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the email, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.

Email can form a contractual obligation

Agreements entered into by email can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

Email systems are commonly used to store information which should be stored somewhere else

All attachments in email should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Employers must be careful how they monitor email

Any employer has a right to monitor the use of email provided it has informed members of staff that it may do so and has obtained consent up front. Monitoring will be carried out by the IT manager, data protection officer (DPO) and/or the vice-principals. If you have used a personal email address to communicate with other members of staff, this could become problematic, as your private email log

will be published as part of an investigation following a data protection breach or audit trail purposes.

Email is one of the most common causes of stress in the work-place

Whilst email can be used to bully or harass people, it is more often the sheer volume of email which causes individuals to feel that they have lost control of their email and their workload. Regular filing and deletion can not only prevent this happening but is expected so that a history-of-emails log can be provided to the DPO when a data breach had occurred or audit trail purposes.

Creating and sending email

Here are some steps to consider when sending email.

- *Do I need to send this e-mail?*
Ask yourself whether this transaction needs to be done by email? It may be that it is more appropriate to use the telephone or to check with someone face to face.
- *To whom do I need to send this email?*
Limit recipients to the people who really need to receive the email. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on received chain emails. When sending emails containing personal or sensitive data always respond to an authorised, approved address (e.g. using our SchoolBase data system to send emails to pupils, parents/guardians or other staff would ensure that only authorised individuals are emailed with regards a pupil). All emails that are used for **official business** must be sent from an official business domain address and **not a personal email address**.
- *Use a consistent method of defining a subject line*
Having a clearly defined subject line helps the recipient to sort the email on receipt. A clear subject line also assists in filing all emails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.
- *Ensure that the e-mail is clearly written*
 - Do not use text language or informal language in school emails.
 - Always sign off with a name (and contact details).
 - Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
 - Never write a whole email in capital letters. This can be interpreted as shouting.
 - Always spell check an email before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
 - If possible, try to stick to one subject for the content of each email, as it will be easier to categorise it later if you need to keep the email.
- *Sending attachments*
Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive (e.g. *dropbox* or *icloud*) and send the link round to the members of staff who need to access it.
- *Disclaimers*
Adding a disclaimer to an email mitigates risk, such as sending information to the wrong recipient, or helps to clarify the college's position in relation to the information being emailed. Typically, they cover the fact that information may be confidential, the intention of

being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the College. The official College disclaimer should be used to ensure it meets our legal obligations.

- *Managing received emails*

This section contains some hints and tips about how to manage incoming e-mails.

- Manage interruptions Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.
 - Turn off any alert that informs you e-mail has been received
 - Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).
- Use rules and alerts. By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:
 - Emails relating to a specific subject or project can be diverted to a named project folder
 - Emails from individuals can be diverted to a specific folder
 - Warn senders that you will assume that if you are copied in to an e-mail, the message is for information only and requires no response from you.
 - Internally, use the following non-definitive list of defined words to indicate in the subject line what is expected of recipients (e.g. "For Action:", FYI:", ask a question, give a command, make an announcement, topic, and so on)
 - Use electronic calendars to invite people to meetings rather than sending e-mails asking them to attend
- Using an out of office message If you check your email at stated periods during the day you can use an automated response to incoming email which tells the recipient when they might expect a reply. A sample message might read as follows: Thank you for your email. I will be checking my email at three times today, 8:30am, 1:30pm and 3:30pm. If you require an immediate response to your email please telephone me on xxxxxxxx. This gives the sender the option to contact you by phone if they need an immediate response.
- Filing email attachments only. Where the main purpose of the email is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The email can then be deleted.
- Email text and attachments. Where the text of the email adds to the context or value of the attached documents it may be necessary to keep the whole email. The best way to do this and retain information which makes up the audit trail, is to save the email in .msg format. This can be done either by clicking and dragging the email into the appropriate folder in an application such as MS Outlook, or by using the "save as" function to save the email in an electronic filing system. If the email needs to be resent it will automatically open into MS Outlook. Where appropriate the email and the attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the email in .msg format will.
- Email text only. If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes. Alternatively the email can be saved in .html or .txt format. This will save all the text in the email and a limited amount of the audit information. The email cannot be resent if it

is saved in this format. The technical details about how to undertake all of these functions are available in application Help functions.

How long to keep emails?

Email is primarily a communications tool, and email applications are not designed for keeping email as a record in a storage area, meeting records management storage standards. Email that needs to be kept should be identified by content: for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these emails will then correspond with the classes of records according to content in the **retention schedule** the College (see appendix 6). These emails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Sending information by post

As College we will routinely send letters containing personal information to our parents or guardians and pupils for example termly reports. However, whilst this is routine, care must still be taken to ensure that the information is correctly addressed to a named recipient and information is not sent in error to the wrong recipient. Mail going to the wrong person is a danger to the individual whose information is being sent. It also puts the College at risk of breaching our responsibilities under the DPA.

You, as the sender, are responsible for making sure that:

- The postal address is correct
- The envelope is clearly marked for the attention of the intended recipient
- No information relating to another pupil has been included in error, either in a letter, email or an attached document
- That you choose the most appropriate method of transfer

Telephone / mobile phone

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, care must be taken as follows:

- Controlled data must not be transferred / discussed over the telephone unless you have confirmed the identity and authorisation of the recipient
- When using answer phones do not leave sensitive or confidential messages, or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing

APPENDIX 5. E-SAFETY

Aims

David Game College aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, proprietors and parents or guardians
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for colleges on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the [National Curriculum computing programmes of study](#).

Roles and responsibilities

The proprietor

The proprietor has overall responsibility for monitoring this policy and holding the principal and vice principals to account for its implementation.

The proprietor will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL) who is Nedaa Belal dsl@davidgamecollege.com.

The proprietor who oversees online safety...

All proprietors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on **acceptable use agreement** (to be signed by all staff members) of the College's ICT systems and the internet (see pro forma 2)

The principal

The principal and vice-principals are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

The designated safeguarding lead

Details of the College's designated safeguarding lead (DSL) and deputy, rachelsherman@davidgame-group.com as well as potentially our **designated prevent lead**, John Dalton (johndaltonlsp@gmail.com), are set out in our **child protection and safeguarding policy** also our **prevent policy**.

The DSL takes lead responsibility for online safety in College, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the college

- Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see pro forma 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College's **behaviour policy**
- Updating and delivering staff training on online safety (pro forma 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to the principal and/or vice-principals

This list is not intended to be exhaustive.

The ICT manager

The ICT manager, Zed Abaderash, zed@davidgamecollege.com and his deputy our data protection officer (DPO), Alexandra Raen, dpo@davidgamecollege.com are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see pro forma 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College's **behaviour policy**

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the College's ICT systems and the internet (pro forma 2), and ensuring that pupils follow the College's terms on **acceptable use agreement** (pro forma 1)
- Working with the DSL and/or **prevent lead** to ensure that any online safety incidents are logged (see pro forma 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College's **behaviour policy**

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff, principal or vice-principals of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on **acceptable use agreement** of the College's ICT systems and internet (pro forma 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

Visitors and members of the community

Visitors and members of the community who use the College's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on **acceptable use agreement** (pro forma 2).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The College will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

The College will raise parents' awareness of internet safety in letters or other communications home and via the SchoolBase notice board in information via our website portal. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal and/or the DSL and prevent lead.

Concerns or queries about this policy can be raised with any member of staff or the principal or vice-principals.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the College's behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The College will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Head of Years and Personal Tutors will discuss cyber-bullying with their pupils and tutees, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, proprietors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The College also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College's **behaviour policy**. Where illegal, inappropriate or harmful material has been spread among pupils, the College will use all reasonable endeavours to ensure the incident is contained.

The DSL or prevent lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, prevent lead or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the College's complaints procedure.

Sexting

Definition

Sexting is when someone has received or sent explicit images, videos or messages. (See also the College's behaviour policy.)

Preventing and addressing sexting

All staff members and volunteers should be aware of the dangers and signs of sexting. If they have any concerns or become aware of young people sharing explicit images or videos of themselves or others should follow the guidance as set out by the NSPCC: <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/sexting-advice-professionals/>

Phishing and Pharming

Definition

A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic looking, albeit fake, web page. The target is asked to input information like a username and password, or even additional financial or personal data.

The miscreant that orchestrates the phishing scheme is able to capture this information and use it to further criminal activity, like theft from a financial account and similar types of criminal activity.

The College has no intention of changing its financial information, therefore never accept an email with a link pretending to be the College's accounts department.

Top tips:

- Never click on hyperlinks in email from an unknown sender, rather manually type the URL into the web browser itself
- Never enter sensitive information in a pop-up window except at those sites that an individual knows to be trustworthy
- Verify HTTPS on the address bar - whenever a person is conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S" confirms that the data is being conveyed through a legitimate, secured channel
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers

- **Education on phishing and pharming attacks** - staying abreast of phishing scams and the technology and techniques designed to prevent them is crucial. A plethora of reliable educational resources exist on the Internet that are designed to assist a person in preventing phishing attacks including a [training course here](#)
- Report phishing and pharming to the financial institution, the [FTC](#), and the [Internet Crime Complaint Centre](#)

Characteristics of a strong password

- At least 8 characters – the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]

Note: do not use < or > in your password, as both can cause problems in web browsers

A strong password is hard to guess, but it should be easy for you to remember – a password that has to be written down is not strong, no matter how many of the above characteristics are employed.

Acceptable use of the internet in the College

All pupils, parents, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of the College's ICT systems and the internet (pro forma 1 and 2). Visitors will be expected to read and agree to the College's terms on acceptable use if relevant.

Use of the College's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, proprietors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the **acceptable use agreements** in pro forma 1 and 2.

Pupils using mobile devices in the College

Pupils may bring mobile devices into the College, but are not permitted to use them during:

- Lessons
- Personal Tutor time
- Clubs on the premises, or any other activities organised by the College

Any use of mobile devices in the College by pupils must be in line with the **acceptable use agreement** (see pro forma 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the College's **behaviour policy**, which may result in the confiscation of their device.

Staff using work devices outside the College

Staff members using a work device outside the College must not install any unauthorised software on the device and must not use the device in any way which would violate the College's terms of **acceptable use agreement**, as set out in pro forma 2.

Staff must ensure that their work device is secure and password-protected with a strong password, so too their online login details to SchoolBase, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of the College. Any USB devices containing data relating to the College must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

How the College will respond to issues of misuse

Where a pupil misuses the College's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the College's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The College will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including **cyber-bullying** and the risks of **online radicalisation**.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e- bulletins and staff meetings).

The DSL, deputy and prevent lead will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Proprietors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy as well as the prevent policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in pro forma 4.

This policy will be reviewed annually by the DSL and prevent lead. At every review, the policy will be shared with the principal and proprietors.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Prevent policy
- Behaviour policy
- Staff disciplinary procedures
- Privacy notices
- Complaints procedure
- Information audit procedure

Pro Forma 1: acceptable use agreement (pupils and parents/guardians/carers)

| | |
|---|-------|
| Acceptable use of the College's ICT systems and internet: agreement for pupils and parents/guardians/carers | |
| Name of pupil: | |
| When using College's ICT systems and accessing the internet in the College, I will not: | |
| <ul style="list-style-type: none"> • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the College's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/guardian/carer • Arrange to meet anyone offline without first consulting my parent/guardian/carer, or without adult supervision | |
| If I bring a personal mobile phone or other personal electronic device into the College: | |
| <ul style="list-style-type: none"> • I will not use it during lessons, tutor group time, clubs or other activities organised by the College, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online | |
| I agree that the College will monitor the websites I visit. | |
| I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. | |
| I will always use the College's ICT systems and internet responsibly. | |
| Signed (pupil): | Date: |
| Parent/carer agreement: I agree that my child can use the College's ICT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for pupils using the College's ICT systems and internet, and for using personal electronic devices in the College, and will make sure my child understands these. | |
| Signed (parent/carer): | Date: |

Pro Forma 2: acceptable use agreement (staff, proprietors, volunteers and visitors)

| | |
|--|-------|
| Acceptable use of the College's ICT systems and the internet: agreement for staff, proprietors, volunteers and visitors | |
| Name of staff member/proprietor/volunteer/visitor: | |
| When using the College's ICT systems and accessing the internet in the College, or outside the College on a work device, I will not: | |
| <ul style="list-style-type: none">• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature• Use them in any way which could harm the College's reputation• Access social networking sites or chat rooms• Use any improper language when communicating online, including in emails or other messaging services• Install any unauthorised software• Share my password with others or log in to the College's network using someone else's details | |
| I will only use the College's ICT systems and access the internet in College, or outside College on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. | |
| I agree that the College will monitor the websites I visit. | |
| I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside College, and keep all data securely stored in accordance with this policy and the College's data protection policy. | |
| I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. | |
| I will always use the College's ICT systems and internet responsibly, and ensure that pupils in my care do so too. | |
| Signed (staff member/proprietor/volunteer/visitor): | Date: |

Pro Forma 3: online safety training needs – self-audit for staff

| Online safety training needs audit | |
|--|-------|
| Name of staff member/volunteer: | Date: |
| Do you know the name of the person who has lead responsibility for online safety in the College? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the College's acceptable use agreement for staff, volunteers, proprietors and visitors? | |
| Are you familiar with the College's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the College's ICT systems and use a strong password? | |
| Are you familiar with the College's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? Please record them here. | |

Pro Forma 4: online safety incident report log

Also see the NSPCC [What to do if a pupil or a teacher reports an e-safety incident](#) flowchart.

| Online safety incident report log | | | | |
|-----------------------------------|-------------------------------|-----------------------------|--------------|---|
| Date | Where the incident took place | Description of the incident | Action taken | Name and signature of staff member recording the incident |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

APPENDIX 6. DATA RETENTION SCHEDULE

Scope: This policy applies to all records created, received or maintained by staff at the college in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by the college and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically. A small percentage of the College's records will be selected for permanent preservation as part of the institution's archives and for historical research.

Responsibilities

David Game College has a responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The proprietor has overall responsibility for this policy. The data protection officer (DPO) primarily responsible for records management in the College will give guidance for good records management practice as is documented in the **data protection policy** and **records management policy**, and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely. Individual members of staff must ensure that records for which they are responsible (see **information audit policy** for a list of who is responsible for what information and records) are accurate, and are maintained and disposed of in accordance with the College's records management guidelines.

Relationship with Existing Policies: This policy has been drawn up within the context of: Freedom of Information Act (FoIA) 2000 and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the College.

Safe Disposal of Records: Where records have been identified for destruction they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information, should be shredded before disposal using a cross cut shredder. Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in the dustbin or a skip. There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way. The FoIA 2000 requires the College to maintain a list or log of records which have been destroyed and who authorised their destruction (see **information audit policy** for a pro forma). This policy also takes into account general data protection regulations (GDPR).

Members of staff should record at least (see **data management policy** for a full breakdown of the required procedure):

- File reference (or another unique identifier)
- File title (or brief description) and number of files
- The name of the authorising officer and the date action was taken. This should be kept in an Excel spreadsheet or similar suitable format

Transfer of Information: Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media. The lifespan of the media and the ability to migrate data where necessary should always be considered (see **data management policy** for a full breakdown of the required procedure).

College Closures and Transfer of Proprietorship: Should the College close or transfer proprietorship there will be records which will need to be stored until they work out their statutory retention periods (see **data management policy** for a full breakdown of the required procedure).

Retention Guidelines: The following retention guidelines have been issued by the Management Society of Great Britain ‘Retention Guidelines for Colleges’.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000. Managing record series using these retention guidelines will be deemed to be ‘normal processing’ under the legislation mentioned above.

If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be **documented**.

The following retention guidelines are also informed by GDPR guidelines.

WHERE APPLICABLE THE FOLLOWING TABLES REGARDING RETENTION OF DATE APPLY

| Child Protection | | | | | |
|---|-----------------------------------|---|----------------------------|---|--|
| <i>Basic file description</i> | Data Protection Issues and | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| <i>Child Protection files Sensitive information</i> | Yes | Education Act 2002, related guidance “Safeguarding Children in Education”, September 2004 | Date of leaving + 25 years | Shred | Child Protection information must be copied and sent under separate cover to new college whilst the child is still under 18 (the information does not need to be sent to a university) Where a child is removed from roll to be educated at home, the file should be copied to the Local Authority. |

| | | | | | |
|--|-----|---|---|-------|--|
| Allegation of a child protection nature against a member of staff, including where the allegation is unfounded | Yes | Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005 | Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer | Shred | <p>The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60:</p> <p>"Record Keeping</p> <p>5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future DBS Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time.</p> <p>The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."</p> |
|--|-----|---|---|-------|--|

| Proprietor | | | | | |
|-----------------------------------|-------------------------------|-----------------------------|---------------------------|---|----------------------|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Principal set of Minutes (signed) | No | | Permanent | Retain in college for 6 years from date of meeting | Transfer to Archives |
| Inspection copies | No | | Date of meeting + 3 years | SHRED | |
| Agendas | No | | Date of meeting | SHRED | |
| Reports | No | | Date of report + 6 years | Retain in college for 6 years from date of meeting | Transfer to Archives |

| | | | | | |
|---|-----|--|--|---|--|
| Annual Parents' meeting papers | No | | Date of meeting + 6 years | Retain in college for 6 years from date of meeting | Transfer to Archives |
| Instruments of Government | No | | Permanent | Retain in college | Transfer to Archives when the college has closed |
| Action Plans | No | | Date of action plan + 3 years | SHRED | It may be appropriate to offer to the Archives |
| Policy documents | No | | Expiry of policy | Retain in college whilst policy is operational | Transfer to Archives |
| Complaints files | Yes | | Date of resolution of complaint + 6 years | Retain in college for the first six years Review for further retention in the case of contentious disputes SHRED routine complaints | |
| Annual Reports required by the Department for Education and Skills | No | | Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171 | Date of report + 10 years | Transfer to Archives |
| Proposals for colleges to become, or be established as Specialist Status colleges | No | | | Current year + 3 years | Transfer to Archives |

| Management | | | | | |
|-------------------------------|-------------------------------|-----------------------------|--|--|--------------------------|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Log Books | Yes | | Date of last entry in the book + 6 years | Retain in the college for 6 years from the date of the last entry. | Transfer to the Archives |

| | | | | | |
|---|-----|--|----------------------------------|--|--------------------------|
| Minutes of the Senior Leadership Team and other internal administrative bodies | Yes | | Date of meeting + 5 years | Retain in the college for 5 years from meeting | Transfer to the Archives |
| Reports made by the principal or the leadership team | Yes | | Date of report + 3 years | Retain in the college for 3 years from meeting | Transfer to the Archives |
| Records created by principal, vice principals, heads of year and other members of staff with administrative responsibilities | Yes | | Closure of file + 6 years | SHRED | |
| Correspondence created by principal, vice principals, heads of year and other members of staff with administrative responsibilities | Yes | | Date of correspondence + 3 years | SHRED | |
| Professional development plans | Yes | | Closure + 6 years | SHRED | |
| College development plans | No | | Closure + 6 years | Review | Offer to the Archives |
| Admissions – if the admission is successful | Yes | | DOB of the pupil + 25 years | SHRED | |
| Admissions – if the appeal is unsuccessful | Yes | | Resolution of case + 1 year | SHRED | |
| Admissions – Secondary Age – Casual | Yes | | Current year + 1 year | SHRED | |

| Pupils | | | | | |
|---|-------------------------------|-----------------------------|--|--|--|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Admission Registers | Yes | | Date of last entry in the book (or file) + 6 years | Retain in the college for 6 years from the date of the last entry. | Transfer to the Archives |
| Attendance Registers | Yes | | Date of register + 3 years | SHRED | |
| Pupil record cards Secondary Age | Yes | Limitation Act 1980 | DOB of the pupil + 25 years | SHRED | |
| Pupil files Secondary Age | Yes | Limitation Act 1980 | DOB of the pupil + 25 years | SHRED | |
| Special Educational Needs files, reviews and Individual Education Plans | Yes | | DOB of the pupil + 25 years | SHRED | |
| Absence books | | | Current year + 6 years | SHRED | |
| Examination results | Yes | | | | |
| Public examination results | No | | Year of examinations + 6 years | SHRED | Unclaimed certificates returned to Exam Board |
| Internal examination results | Yes | | Current year + 5 years | SHRED | |

| Pupils | | | | |
|--|-------------------------------|---------------------------------------|---|--|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record |
| Any other records created in the course of contact with pupils | Yes/No | | Current year + 3 years | Review at the end of 3 years and either allocate a further retention period or SHRED |
| Statement maintained under The Education Act 1996 - Section 324 | Yes | SEN and Disability Act 2001 Section 1 | DOB + 30 years | SHRED unless legal action is pending |
| Proposed statement or amended statement | Yes | SEN and Disability Act 2001 Section 1 | DOB + 30 years | SHRED unless legal action is pending |
| Advice and information to parents regarding educational needs | Yes | SEN and Disability Act 2001 Section 1 | Closure + 12 years | SHRED unless legal action is pending |
| Accessibility Strategy | Yes | SEN and Disability Act 2001 Section 1 | Closure + 12 years | SHRED unless legal action is pending |
| Children's SEN Files | Yes | | DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases | SHRED unless legal action is pending |
| Parental permission slips for college trips – where there has been no major incident | Yes | | Conclusion of the trip | SHRED |
| Parental permission slips for college trips – where there has been a major incident | Yes | Limitation Act 1980 | DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils | SHRED |

| | | | | |
|---|----|---|--------------------------|-------|
| Records created by colleges to obtain approval to run an Educational Visit outside the Classroom - Secondary Age Colleges | No | 3 part supplement to the H&S of Pupils on Educational Visits (HASPEV) (1998). | Date of visit + 10 years | SHRED |
|---|----|---|--------------------------|-------|

| Curriculum | | | | |
|-------------------------------|-------------------------------|-----------------------------|-------------------------|--|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record |
| Curriculum development | No | | Current year + 6 years | SHRED |
| Curriculum returns | No | | Current year + 3 years | SHRED |
| College syllabus | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| Schemes of work | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| Timetable | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| Class record books | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| Mark Books | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| Record of homework set | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| Pupils' work | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |

| | | | | |
|---------------------|-----|--|------------------------|-------|
| Examination results | Yes | | Current year + 6 years | SHRED |
| SATS records | Yes | | Current year + 6 years | SHRED |
| PAN reports | Yes | | Current year + 6 years | SHRED |
| Value added records | Yes | | Current year + 6 years | SHRED |

| Staff records | | | | |
|--|------------------------|--|--|--|
| Basic file description | Data Protection | Statutory Provisions | Retention Period | Action at the end of the administrative |
| Timesheets, sick pay | Yes | Financial Regulations | Current year + 6 years | SHRED |
| Staff Personal files | Yes | | Termination + 7 years | SHRED |
| Interview notes and recruitment | Yes | | Date of interview + 6 months | SHRED |
| Pre-employment vetting information (including DBS) | No | DBS guidelines | Date of check + 6 months | SHRED |
| Disciplinary proceedings: | Yes | Where the warning relates to child protection issues then retain until the person's normal retirement age, or 10 years from the date of the allegation, whichever is the longer If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice. | | |
| • oral warning | | | Date of warning + 6 months | SHRED |
| • written warning – level one | | | Date of warning + 6 months | SHRED |
| • written warning – level two | | | Date of warning + 12 months | SHRED |
| • final warning | | | Date of warning + 18 months | SHRED |
| • case not found | | | If child protection related then retain until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer. | SHRED |
| Records relating to accident/injury at work | Yes | | Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied | SHRED |

| | | | | |
|--|-----|---|--|-------|
| Annual appraisal/assessment | No | | Current year + 5 years | SHRED |
| Salary cards | Yes | | Last date of employment + 85 years | SHRED |
| Maternity pay records | Yes | Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567) | Current year, + 3yrs | SHRED |
| Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Yes | | Current year + 6 years | SHRED |
| Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure | Yes | | Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file. | |

| Health and Safety | | | | |
|-------------------------------|-------------------------------|--|---|---|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record |
| Accessibility Plans | | Disability Discrimination Act | Current year + 6 years | SHRED |
| Accident Reporting | | Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 | | |
| Adults | Yes | | Date of incident + 7 years | SHRED |
| Children | Yes | | DOB of child + 25 years | SHRED |
| COSHH | | | Current year + 10 years [where appropriate an additional retention period may be allocated] | SHRED |

| | | | | |
|---|-----|--|-------------------------|-------|
| Incident reports | Yes | | Current year + 20 years | SHRED |
| Policy Statements | | | Date of expiry + 1 year | SHRED |
| Risk Assessments | | | Current year + 3 years | SHRED |
| Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos | | | Last action + 40 years | SHRED |
| Process of monitoring of areas where employees and persons are likely to have come in contact with radiation | | | Last action + 50 years | SHRED |
| Fire Precautions log books | | | Current year + 6 years | SHRED |

| Administrative | | | | | |
|----------------------------------|-------------------------------|-----------------------------|-----------------------------|---|----------------------|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Employer's Liability certificate | | | Closure of the college + 40 | SHRED | |
| Inventories of equipment and | | | Current year + 6 years | SHRED | |
| General file series | | | Current year + 5 years | Review to see whether a further retention period is | Transfer to Archives |
| College brochure or prospectus | | | Current year + 3 years | | Transfer to Archives |
| Circulars (staff/parents/pupils) | | | Current year + 1 year | SHRED | |
| Newsletters, ephemera | | | Current year + 1 year | Review to see whether a further retention period is | Transfer to Archives |
| Visitors' book | | | Current year + 2 years | Review to see whether a further retention period is | Transfer to Archives |
| PTA/Old Pupils Associations | | | Current year + 6 years | Review to see whether a further retention period is | Transfer to Archives |

| Finance | | | | | |
|------------------------------|------------------------|-----------------------|---|--|---|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Annual Accounts | | Financial Regulations | Current year + 6 years | Offer to the Archives | Annual Accounts |
| Loans and grants | | Financial Regulations | Date of last payment on loan + 12 years | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Contracts under seal | | | Contract completion date + 12 years | SHRED | |
| Contracts under signature | | | Contract completion date + 6 years | SHRED | |
| Contracts monitoring records | | | Current year + 2 years | SHRED | |

| Finance | | | | | |
|--|------------------------|-----------------------|------------------------|--|--|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Copy orders | | | Current year + 2 years | SHRED | |
| Budget reports, budget monitoring etc. | | | Current year + 3 years | SHRED | |
| Invoice, receipts and other records covered by the Financial Regulations | | Financial Regulations | Current year + 6 years | SHRED | |
| Annual Budget and background | | | Current year + 6 years | SHRED | |
| Order books and requisitions | | | Current year + 6 years | SHRED | |
| Delivery Documentation | | | Current year + 6 years | SHRED | |
| Debtors' Records | | Limitation Act 1980 | Current year + 6 years | SHRED | |
| College Fund – Cheque books | | | Current year + 3 years | SHRED | |

| | | | | | |
|---|-----|-----------------------|------------------------------------|-------|--|
| College Fund – Paying in books | | | Current year + 6 years then review | SHRED | |
| College Fund – Ledger | | | Current year + 6 years then | SHRED | |
| College Fund – Invoices | | | Current year + 6 years then | SHRED | |
| College Fund – Receipts | | | Current year + 6 years | SHRED | |
| College Fund – Bank statements | | | Current year + 6 years then | SHRED | |
| College Fund – College Journey | | | Current year + 6 years then | SHRED | |
| Applications for free college meals, travel, uniforms etc | | | Whilst child at college | SHRED | |
| Student grant applications | | | Current year + 3 years | SHRED | |
| Free college meals registers | Yes | Financial Regulations | Current year + 6 years | SHRED | |
| Petty cash books | | Financial Regulations | Current year + 6 years | SHRED | |

| Property | | | | | |
|--|-------------------------------|-----------------------------|---------------------------|---|-------------------|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Plans | | | Permanent | Retain in college whilst operational | Offer to Archives |
| Maintenance and contractors | | Financial Regulations | Current year + 6 years | SHRED | |
| Leases | | | Expiry of lease + 6 years | SHRED | |
| Lettings | | | Current year + 3 years | SHRED | |
| Burglary, theft and vandalism report forms | | | Current year + 6 years | SHRED | |
| Maintenance log books | | | Last entry + 10 years | SHRED | |
| Contractors' Reports | | | Current year + 6 years | SHRED | |

| Local Authority | | | | | |
|---|-------------------------------|-----------------------------|-------------------------------|---|---------------------|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Secondary Age transfer sheets (Primary) | Yes | | Current year + 2 years | SHRED | |
| Attendance returns | Yes | | Current year + 1 year | SHRED | |
| Circulars from LA | | | Whilst required operationally | Review to see whether a further retention period is required | Transfer to Archive |

| Department for Education | | | | | |
|---|-------------------------------|-----------------------------|--|---|----------------------|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| HMI reports | | | These do not need to be kept any longer | | Transfer to Archives |
| OFSTED reports and papers | | | Replace former report with any new inspection report | Review to see whether a further retention period is required | Transfer to Archives |
| Returns | | | Current year + 6 years | SHRED | |
| Circulars from Department for Education | | | Whilst operationally required | Review to see whether a further retention period is required | Transfer to Archives |

| Connexions / Prospects | | | | | |
|-------------------------------|-------------------------------|-----------------------------|-------------------------|---|--|
| Basic file description | Data Protection Issues | Statutory Provisions | Retention Period | Action at the end of the administrative life of the record | |
| Service level agreements | | | Until superseded | SHRED | |
| Work Experience agreement | | | DOB of child + 18 years | SHRED | |

| Other Records - Administration | | | |
|---|------------------------|--|--|
| Basic file description | Data Protection | Statutory Provisions | Retention Period |
| Financial Records | | | |
| Financial records – accounts, statements, invoices, petty cash etc | No | | Current year + 6 years |
| Insurance | | | |
| Insurance policies – Employers Liability | No | Employers Liability Financial Regulations | The policies are kept for a minimum of 6 years and a maximum of 40 years depending on the type of policy |
| Claims made against insurance policies – damage to property | Yes | | Case concluded + 3 years |
| Claims made against insurance policies – personal injury | Yes | | Case concluded + 6 years |
| Human Resources | | | |
| Personal Files - records relating to an individual's employment history | Yes**1 | | Termination + 6 years then review |
| Pre-employment vetting information (including DBS checks) | No | DBS guidelines | Date of check + 6 months |
| Staff training records – general | Yes | | Current year + 2 years |
| Training (proof of completion such as certificates, awards, exam | Yes | | Last action + 7 years |
| Premises files (relating to maintenance) | No | | Cessation of use of building + 7 years then |
| Risk Assessments | No | | Current year + 3 years |

1

**For Data Protection purposes the following information should be kept on the file for the

| | |
|---|------------------------|
| All documentation on the personal file | Duration of employment |
| Pre-employment and vetting information | Start date + 6 months |
| Records relating to accident or injury at work | Minimum of 12 years |
| Annual appraisal/assessment records | Minimum of 5 years |
| Records relating to disciplinary matters (kept on personal files) | |
| • oral warning | 6 months |
| • first level warning | 6 months |
| • second level warning | 12 months |
| • final warning | 18 months |

| | | | |
|--|-----|--|---|
| Staff training records – general | Yes | | Current year + 2 years |
| Training (proof of completion such as certificates, awards, exam | Yes | | Last action + 7 years |
| Premises and Health and Safety | | | |
| Premises files (relating to maintenance) | New | | Cessation of use of building + 7 years then |
| Risk Assessments | New | | Current year + 3 years |

The following items apply to DGHE only:

| RECORD GROUP | RETENTION PERIOD |
|---|--|
| Records documenting the enquiries made by members of the public for the provision of our educational services | Date of initial enquiry + 1 year |
| Records documenting the handling of applications for admission: successful applications. | End of student relationship + 6 years |
| Records documenting the handling of applications for admission: unsuccessful applications. | Completion of admissions process + 1 year. |
| Records containing personal data on individual students | Minimum requirement varies for different types of personal data. Recommended <u>maximum</u> retention: End of 'registered student' relationship with institution + 6 years |
| Records documenting the withdrawal of individual students from the institution. | Termination of relationship with student + 6 years |
| Records documenting the termination of individual students' programmes. | Termination of relationship with student + 6 years |
| Records documenting the conduct and results of disciplinary proceedings against individual students. | Last action on case + 6 years |
| Records documenting the handling and results of academic appeals by individual students. | Last action on case + 6 years |
| Records documenting the handling of formal complaints made by individual students against the institution. | Last action on case + 6 years |
| Records documenting the handling of complaints by individual students where the formal complaints procedure is not initiated. | Last action on complaint + 3 years |
| Records documenting individual students' attendance at examinations, and the handling of reports of mitigating circumstances. | Current academic year + 1 year |
| Records documenting individual students' submission of assessed work and handling of reports of mitigating circumstances. | Current academic year + 1 year |
| Records documenting the handling of applications for remission of tuition fees: successful applications. | Determination of application + 6 years |
| Records documenting the handling of applications for remission of tuition fees: unsuccessful applications. | Determination of application + 1 year |

Last reviewed: April 2018 (A.Raen) Previous review: January 2018 (J. Sanders)