GDPR and Data Protection Policy

Date Published	February 2020
Next Review	February 2021
UCC Governor Approval Committee	*Resources*
UCC Staff Role Responsible	Data Compliance Manager (DPO Liaison)

UCC Data Protection Policy	
CONTENT	PAGE

1. Aims

At Uppingham Community College, we are committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data – and that is a personal responsibility that we take very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in line with the requirements and protections set out in the General Data Protection Regulation.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

The General Data Protection Regulation (GDPR) is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA), in May 2018. It was necessary, as the old Data Protection Act had been in force for 20 years. Over time, technological advances meant that the law protecting individuals had to be updated.

The GDPR and DPA 2018 exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The GDPR exists to protect individual rights in an increasingly digital world.

3. Who does it apply to?

Everyone, including schools. As Public bodies schools have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the new Act.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

4. What is Data?

Any information that relates to a living person that identifies them. This can be name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethical origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Every school also has to publish a Privacy / Fair Processing Notice on the website.

5. What are the Key Principles of the GDPR

Lawfulness, transparency and fairness.

School must have a legitimate reason to hold the data; we explain this in the Data Privacy Notices on the website. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent as explained in 'Data Subjects Rights'.

Collect data for a specific purpose and use it for that purpose

So data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack, only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller, in any event a dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention

School has a retention policy that explains how long we store records for; this is available on request.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information.

6. What is a 'data subject'?

Someone whose details we keep on file. Some details are more sensitive than others. The GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

7. Subject Access Requests

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays. The maximum extension is up to two months.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy and later information in this DPA policy.

8. Who is a 'data controller'?

Our school is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

9. Who is the 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data
School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The GDPR has six conditions for lawful processing and any time we process data relating to an individual, it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

10. Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

11. Breaches and Non-Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed (Appendix 1).

Protecting data and maintaining data subjects rights is the purpose of this policy and associated procedures.

The school 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 a school context may include, but are not limited to:

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

12. Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the school website, we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On arrival at school, you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. (A form is available)

Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupil's may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

13. Biometrics

The school operates biometric recognition systems for:

- registration
- purchasing food in the canteen
- library

All data collected will be processed in accordance with the GDPR Data Protection Principles and the Protection of Freedoms Act 2012. The written consent of at least one parent will be obtained before biometric data is taken and used. If one parent objects in writing, then the school will not take or use a child's biometric data.

For more information about biometric data please refer to the ICO Guidance at the link below:

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

14. CCTV

Please also see the CCTV Policy

We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behaviour and exclusion management processes
- To assist the school in complying with legal and regulatory obligations

Enquiries about the CCTV system should be directed to the Site Manager: Berridge_s@ucc.rutland.sch.uk

15. Data Protection Officer

We have a Data Protection Officer whose role is to:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA

- to provide advice where requested about the data protection impact assessment and monitor its performance
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

The Data Compliance Manager is responsible for overseeing the implementation of this policy within the college, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The Data Compliance Manager is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our Data Compliance Manager is contactable at DCM@ucc.rutland.sch.uk who will liaise with the DPO. Our DPO is John Walker Solicitor, J.A. Walker Solicitors at info@jawalker.co.uk

16. Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

- All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

17. Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDRP and DPA compliance.
Stone Group Recycling are responsible for; hardware disposal, hardware recycling, server and hard drive cleansed, destroying of portable and removable storage.
We have used a company called Conserve IT in the past and this year we are trialling Stone Group Recycling. We always use WEEE compliant recycling facilities, as it is our legal obligation to dispose of our unused equipment safely and securely.
Any servers, hard drives, removable storage is recycled or destroyed via the recycling company.

Hard copy files are departmentally responsible for destroying sensitive documents.

18. Complaints and the Information Commissioner Office (ICO)

The school Complaints Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form (*Appendix 1, Complaints Policy*), and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

19. Review

The Data Protection Officer and Data Compliance Manager will conduct a review of the effectiveness of GDPR compliance and processes every 12-24 months.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential 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 Data Compliance Manager will alert the headteacher after liaising with the DPO.
- 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 over their data
    - Discrimination
    - Identify 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. A breach log will be kept both within the college and with the DPO, along with breach notification forms and documented decisions.
- 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 data 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 Data Compliance Manager will let the DPO have 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 Data Compliance Manager 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 Data Compliance Manager 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 Data Compliance Manager 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 on the **GDPR Group site on Office 365**
- The Data Compliance Manager will liaise with the DPO and will meet with the Principal 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.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Data Compliance Manager will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Data Compliance Manager will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Data Compliance Manager will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Compliance Manager will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of data breach:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised student exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen